Hochschule Lausitz (FH)

Fachbereich IEM

Studiengang Systems Engineering

Identitätsmanagement an der Hochschulbibliothek der Hochschule Lausitz (FH)

Zugang zu elektronischen Ressourcen der Hochschulbibliothek

Masterarbeit

Wintersemester 2010/2011

von

Tilo Kunze

Geburtsdatum: 09.12.1974
Matrikelnummer: 982461
E-Mail: Tilo.Kunze@HS-Lausitz.de

1. Gutachter: Prof. Dr. Andreas Freytag
2. Gutachter: Prof. Dr. Martin Weigert

Abgabedatum: 15.12.2010
letzte Änderung: 12.12.2010

Tilo Kunze

Wehrstraße 23

01968 Senftenberg

Hiermit versichere ich, dass ich die von mir vorgelegte Arbeit selbstständig verfasst habe, dass ich die verwendeten Quellen, Internet-Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Senftenberg, den 15.12.2010

_____

Tilo Kunze

Inhalt

Verzeichnis der Abbildungen

Verzeichnis der Tabellen

Verzeichnis der Abkürzungen

AAI	Authentifizierungs- und Autorisierungs-Infrastruktur
ADS	Active Directory System
BA	Bachelor (akademischer Grad)
BIX	Bibliotheksindex
DBS	Deutsche Bibliotheksstatistik
DBV	Deutscher Bibliotheksverband
DFN	Deutsches Forschungsnetz
EDUROUM	education roaming
EFRE	Europäischer Fond für regionale Entwicklung
FAK	Friedrich-Althoff-Konsortium
HAN	Hidden Automatic Navigator
HB	Hochschulbibliothek
HIS	Hochschul - Informations - System
HL	Hochschule Lausitz (FH)
HRZ	Hochschulrechenzentrum
HTML	Hypertext Markup Language
IDM	Identitätsmanagement
JDBC	Java Database Connectivity
LBS	Lokales Bibliothekssystem
LDAP	Lightweight Directory Access Protocol
MA	Master (akademischer Grad)
OCLC	Online Computer Library Center
ODBC	Open Database Connectivity
OPAC	Online Public Access Catalogue
SLNP	Simple Library Network Protocol
SQL	Structured Query Language
VM	virtuelle Maschine
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

1 Einleitung

Keine moderne Hochschule kann sich mehr vor dem Informations- und Medienzeitalter und den damit einhergehenden Veränderungen und Herausforderungen verschließen. Besonders die Bereiche Lehre und Verwaltung sind diesem Wandel unterworfen und müssen mit ihren Dienstleistungen und Serviceangeboten darauf reagieren. Neue Studenten stellen mit ihren Anforderungen einen zusätzlichen Motor in diesem Wandel dar. Reagieren die Hochschulen darauf nicht in erforderlichem Maße, wird dies mit sinkenden Studierendenzahlen quittiert werden.

Einen besonderen Schwerpunkt bildet dabei die Sicherung und Verbesserung der Leistungsfähigkeit der Hochschulbibliothek.

Die Hochschulbibliothek ist vom beschriebenen Wandel dreifach betroffen:

1. Sie ist Anlaufpunkt für alle Studierenden und Mitarbeiter und muss alle Fachbereiche (mit den entsprechenden Studiengängen differenziert nach BA- und MA-Level) mit Medien und Informationen versorgen.
2. Sie ist, wie alle Bereiche, den finanziellen und personellen Sparzwängen der Hochschule unterworfen.
3. Sie muss die Informationsversorgung auf elektronische Medien erweitern, ohne dabei auf Bestehendes (Printmedien) zu verzichten.

Alle drei Sachverhalte müssen jedoch im Zusammenhang betrachtet werden.

Die Hochschulbibliothek versorgt als zentrale Serviceeinrichtung der Hochschule Lausitz (FH) die Studierenden, Lehrenden und Mitarbeiter der Verwaltung mit Fachliteratur und -informationen in gedruckter oder digitaler Form. Aber auch jeder Interessierte ab dem 16. Lebensjahr (aus der Region) kann die Hochschulbibliothek kostenlos nutzen.

Die Hochschulbibliothek verzeichnete in den vergangenen drei Jahren einen merklichen Rückgang der Ausleihzahlen. So wurden 2007 noch von jedem Bibliotheksnutzer im Durchschnitt 32 Medien im Jahr ausgeliehen, hingegen waren es 2009 nur noch ca. 27[1]. Als Hauptgrund ist der Erwerb von geringeren Stückzahlen (teilweise können nur noch Präsenzexemplare angeschafft werden) auf Grund des ständig sinkenden Eta zu nennen, was aber auch mit höheren Medienpreisen korreliert.

[1] [HS2010] Statistik Internetseite HS Lausitz Hochschulbibliothek [31.10.2010]

Im gleichen Zeitraum hat sich der Zugriff auf die elektronischen Bücher (E-Books) innerhalb des Campusnetzes von 5.500 Zugriffen auf mehr als 13.000 verdoppelt.

Hieraus lässt sich schlussfolgern, dass die Akzeptanz dieses Mediums gestiegen ist. Hauptgründe dafür sind sicher die stete Verfügbarkeit und die komfortable Recherche im Werk. Kritisiert wird hingegen die erschwerte Lesbarkeit am Bildschirm und die daraus folgende Notwendigkeit eines PC's.[2]

Die Hochschulbibliothek hat sich deshalb dazu entschlossen, weitere 10.000 E-Books im Rahmen einer EFRE-Antragstellung in 2011 zu erwerben. Das entspricht einem Budget von ca. 500 Printmedien (70.000 €)

Des Weiteren muss die Integration der Hochschulbibliothek in die Hochschulverwaltung ausgebaut werden. Das betrifft vor allem den Austausch von Nutzerdaten. Ein dezentrales Identitätsmanagement kann von der Hochschulbibliothek personell nicht getragen werden.

Die Hochschulbibliothek muss ihre Dienstleistungen ortsunabhängig, intuitiv und statistisch belegbar anbieten.

In der vorliegenden Masterarbeit soll deshalb vor allem auf die veränderten Anforderungen an die Hochschulbibliothek eingegangen werden und Lösungsansätze sowie exemplarische Lösungen aufgezeigt werden.

[2] [Springer2008]

2 Anforderungen an ein Identitätsmanagement in Hochschulen

Ein Identitätsmanagement (IDM) stellt eine gesamtheitliche Verwaltung von Identitäten und darauf basierender Berechtigungen dar.[3]

Mit einem IDM sollen organisatorische Prozesse, welche mit der Verwaltung von Personen und Dingen zu tun haben, abgebildet werden. Dies soll die Datenkonsistenz erhöhen und gleichzeitig den Verwaltungsaufwand minimieren. [4]

Mit einem IDM soll erreicht werden, dass Personen

- persönliche Informationen einsehen (z.B. Prüfungsergebnisse)
- persönliche Daten ändern (Namens oder Adressänderungen)
- Identität beweisen (authentifizieren), um Dienste und Ressourcen in Anspruch nehmen zu können.

Organisationen wollen

- Identitätsinformationen über Mitarbeiter oder Studenten verwalten
- Benutzer ihrer Ressourcen verwalten
- Konsistenz der Daten in verschiedenen Informationsspeichern erreichen
- Vortäuschung falscher Identitäten verhindern.

Daraus lassen sich für eine Hochschulbibliothek vor allem zwei Punkte ableiten:

2.1 Konsistenz der Identitätsinformationen von Nutzern

Diese kann man kurz mit „keine doppelte Aufnahme und stetige Aktualität von Nutzerdaten“ umschreiben.

Hierbei stellt die Analyse der vorhandenen, gewollten und evtl. weiterzugebenden Daten einen Schwerpunkt dar.

Viel wichtiger als die technische Lösung dieses Datenabgleichs ist die Frage des Datenschutzes. Es handelt sich hier teilweise um große Datenstämme (Name, Geburtsdatum, Adressdaten, Matrikelnummer, Telefonnummern, E-Mail-Adressen usw.).

[3] [Lee]
[4] [Gietz]

2.2 Verwalten von Zugriffen auf Ressourcen

Nur für berechtigte Nutzer sollen Dienste angeboten und zugelassen werden, z.B. die Ausleihe von Büchern, das Lesen von Zeitschriften, die Nutzung von IuK-Technik, Recherchen in Online-Datenbanken usw.

Auch hier ist eine Analyse notwendig: Um welche Ressourcen handelt es sich (z.B. Drucken, Kopieren, Scannen, Internetrecherche, Zugang zu Datenbanken und E-Books), wie / wann / womit kann darauf zugegriffen werden.

Das Ausleihen von Büchern ist seit den Anfängen der Bibliothek nur mit einer Legitimation möglich. Das Lesen von Zeitschriften vor Ort dagegen ist in den meisten Bibliotheken für jeden Walk-In-User möglich.

Die Bereitstellung moderner Ressourcen, benötigt eine andere Herangehensweise an die berechtigte Nutzung.

Hochschulbibliotheken sind meist in Hochschulnetze eingebunden. Damit müssen die Benutzungsordnungen des Netzbetreibers, meist Hochschulrechenzentren, erfüllt werden. So steht in der Benutzungsordnung[5] des HRZ der Hochschule Lausitz im § 4 „Nutzungsberechtigte und Zulassung zur Nutzung“ folgendes: „Die Zulassung erfolgt ausschließlich zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, für Zwecke der Hochschulbibliothek“ damit übernimmt das HRZ die Empfehlungen des Deutschen Forschungsnetzes (DFN)[6]. Das DFN steht über den Hochschulrechenzentren und stellt den Netzprovider der Hochschulen dar und fungiert in rechtlichen und fachlichen IuK-Fragen als direkter Ansprechpartner für diese Serviceeinrichtungen.

„Zu Zwecken der Bibliothek“ ist eine sehr frei definierbare Aussage. Man sollte hier die traditionellen Werte des Bibliothekswesens, nämlich die freie Meinungsäußerung und der freie Zugang zu Informationen heranziehen. Diese Werte wurden durch das IFLA/UNESCO Internet-Manifest[7] auch in das digitale Zeitalter übernommen und mit „Bibliotheken sollten sicherstellen, dass der Zugang zu Informationen im Netz für alle Benutzer offen steht“ eindeutig beschrieben. Dies geht auch aus der DINI Empfehlung für öffentliche Arbeitsplätze[8] hervor, welche keine Beschränkung des Internets vorsieht und den freien Zugang zu Informationen unterstreicht.

---

5 [HRZ2006]
6 Internet: http://www.dfn.de/rechtimdfn/rgwb/rechtsguide/rg-kapitel1/muster/ [21.11.2010]]
7 [IFLA]
8 [DINI ÖA]

Laut [BibDi2000] wurde bereits im Jahr 2000 empfohlen: „Der uneingeschränkte Zugang zum Internet (nicht Intranet) sollte nur auf dem Wege einer persönlichen Anmeldung, möglich sein.“[9] Auf das Gesetz der Vorratsdatenspeicherung wurde mit der Empfehlung des Deutschen Bibliotheksverbandes[10] (DBV) reagiert. In dieser Empfehlung wird auf die Bildung einer eingeschränkten Nutzergruppe (mit der man davon ausgenommen war, Vorratsdaten zu speichern) hingewiesen und dass das Zugangsrecht nur für diese bereit zu stellen sei. Mit dem „Kippen“ der Vorratsdatenspeicherung wurde diese Bedingung jedoch 2009 (siehe Presseartikel[11]) abgeschwächt. Laut DBV2010[12] kann weiterhin der Internetzugang nur autorisierten Nutzern angeboten werden. Eine Speicherung von Login- und Benutzungsdaten wurde ausdrücklich untersagt. Dadurch entfällt auch die datenschutzrechtliche Problematik bei der Datenspeicherung.

Jeder Benutzer der Bibliothek hat mit einer Authentifizierung freien Internetzugriff. Aber mit der Bereitstellung von erworbenen nicht frei zugänglichen elektronischen Ressourcen sind Lizenzbedingungen zu erfüllen. Diese können sehr unterschiedliche Nutzungsbedingungen aufweisen, wie die beiden nachfolgenden Beispiele zeigen:

Produkt: WISO, FAK-Konsortial-Nutzungsvertrag

„NUTZUNGSRECHTE

[...] das örtlich, auf die Räume der Hochschule, begrenzte (Campuslizenz), nicht ausschließliche Recht ein, die Datenbanken zu wissenschaftlichen Forschungs- und Ausbildungszwecken für ihre Hochschulangehörigen bereitzuhalten […]
GESCHÄFTSBEDINGUNGEN

[...] dieses Angebot im Rahmen seiner Organisation einem hierfür berechtigten Nutzerkreis zur Verfügung zu stellen.“

Produkt: SpringerLink Plattform, Lizenzvertrag

„BERECHTIGTE NUTZER

[...] sind Wissenschaftler, Angestellte und Mitarbeiter der Lizenznehmer sowie Privatpersonen, die die Bibliotheken besuchen und diese zu persönlichen wissenschaftlichen Zwecken nutzen. Nutzungsberechtigt sind auch Personen an Zweig- bzw. Außenstellen, nicht aber Organisationen, Firmen oder Einrichtungen, es sei denn sie sind in Anlage B genannt. Die Präsenznutzung durch Besucher bzw. Nutzer einer Bibliothek erfüllt nicht den Tatbestand der "öffentlichen Wiedergabe" gem. § 4 AOB.“ (AOB = Allgemeine Online-Vertragsbedingungen).

---

9 [BibDi2000] S. 1506
10 [DBV2006]
11 Internet: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011 [12.11.2010]
12 [DBV2010]

Diese zwei Beispiele für die Nutzung elektronischer Medien zeigen auf, dass eine sehr genaue Analyse der Lizenzbedingungen stattfinden muss.

Zusammenfassend ist festzustellen, dass alle Nutzer das Recht auf einen freien Zugang zum Internet, haben aber nicht jeder Nutzer hat das Recht, auch lizenzierte Datenbanken oder andere elektronische Medien frei zu nutzen. Es muss somit eine Authentifizierung des Nutzers stattfinden.

3 Analyse des Ist-Zustandes an der Hochschule Lausitz (FH)

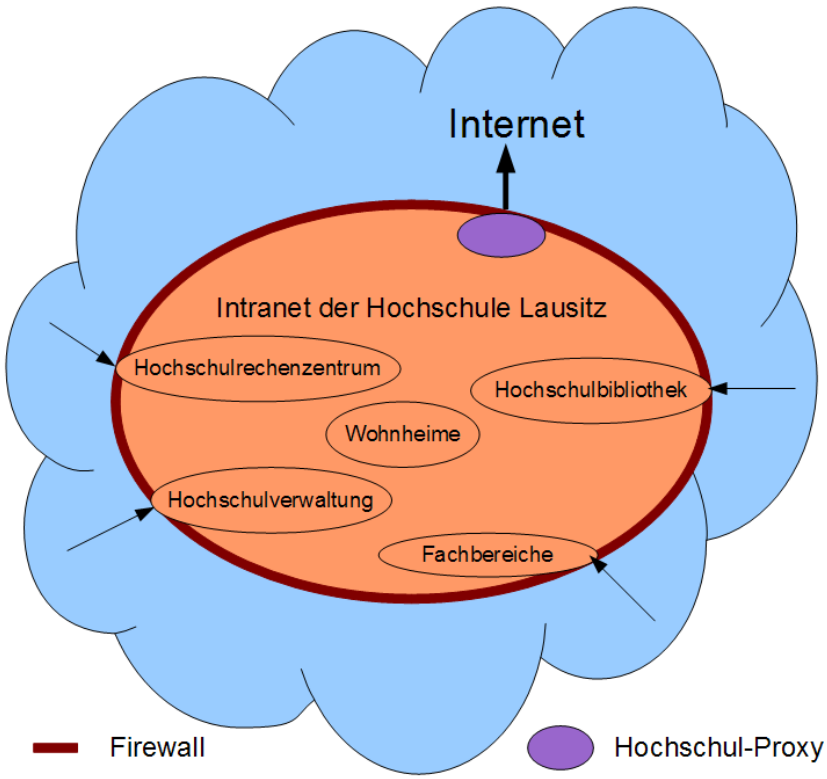

Abb. 1: Schematische Netzwerkübersicht

Abbildung 1 zeigt eine schematische Übersicht über die Campusstruktur der Hochschule Lausitz. Alle Einrichtungen der Hochschule befinden sich im IT-Campusnetzwerk, welches durch das Hochschulrechenzentrum (HRZ) verwaltet wird. Das Hochschulnetz wird durch eine Firewall vom Internet getrennt und geschützt. Der Hochschulproxy stellt dabei die zentrale Schnittstelle zwischen Intranet und Internet dar. Jede Internetanfrage muss über diesen Proxy abgewickelt werden. Anfragen aus dem Internet werden über die Firewall verhindert, bzw. bestimmte Dienste wurden freigegeben, um diese auch vom Internet aus zur Verfügung zu stellen. So ist z.B. der webOpac[13] der Hochschulbibliothek auch vom Internet aus, zu erreichen.

[13] Internet: http://opac.fh-lausitz.de [10.10.2010]

3.1 Nutzerverwaltung

3.1.1 Im Hochschulrechenzentrum (HRZ) bzw. Studentensekretariat

In der Hochschule Lausitz wird die Prüfungsverwaltung (POS), das Studierendenmanagement (SOS), die Zulassungsverwaltung (ZUL), die Finanz- und Sachmittelverwaltung (FSV), das Personalmanagement (SVA), die Kosten- und Leistungsrechnung (COB) und das Gebäude- und Flächenmanagement (BAU) mit Hilfe des Hochschul-Informations-Systems (HIS)[14] durchgeführt. Alle Module speichern ihre Daten in einer komplexen Datenbankstruktur.

Im Jahr 2008 wurde mit Hilfe einer Diplomarbeit[15] eine zentrale Benutzerdatenverwaltung aufgebaut, die durch die einzelnen Module SVA, LSF und SOS der HIS – Verwaltung gespeist werden.

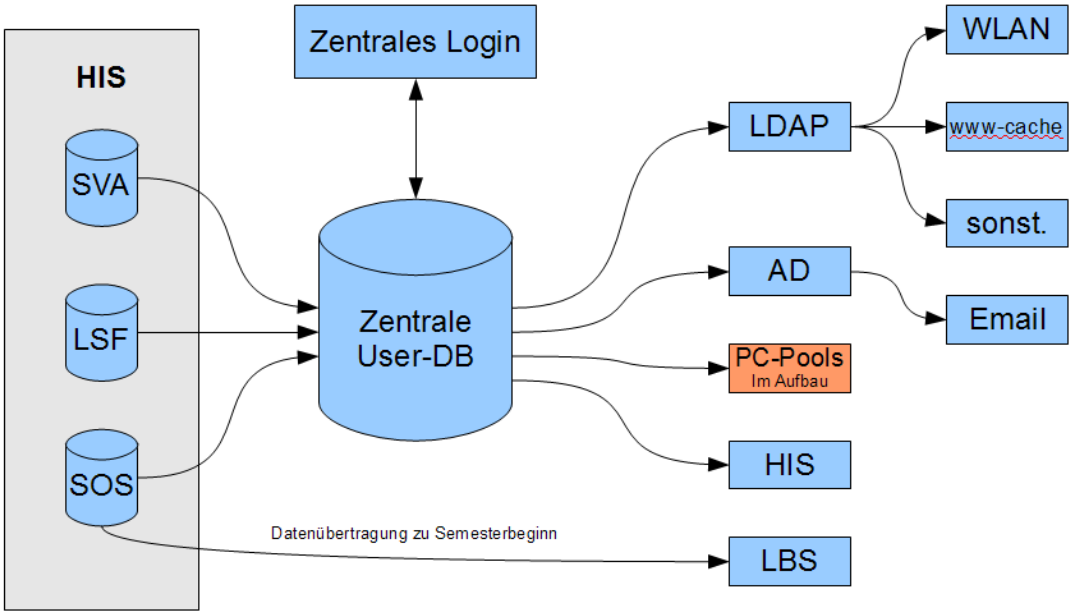

Abb. 2: Schematische Übersicht der IuK- Struktur der HL

Durch eine Studienbewerbung (online oder postalisch) werden Nutzerdaten erstmals im Studentensekretariat aufgenommen, im weiteren Bewerbungsprozess wird eine Immatrikulationsnummer generiert. Diese Daten werden zur zentralen Nutzerdatenbank übertragen. Der Studienanwärter erhält alle benötigten Unterlagen und muss seinen Hochschul- Account über das zentrale Login aktivieren.

[14] Internet: http://www.his.de [20.11.2010]
[15] [Starick]

Studenten haben mit diesem HS- Account derzeit einen Zugang zum:

- Vorlesungs- und Veranstaltungsverzeichnis (HIS-LSF)
- ONLINE- Prüfungsamt (Adressänderung, Prüfungsverwaltung, Notenspiegel)
- HTML-Webspace
- E-Mailkonto der HS Lausitz (Microsoft Exchange Server)
- Proxy-Authentifikation im Wohnheimdatennetz (www-cache)
- WLAN-Zugang an der Hochschule Lausitz
- Authentifizierung an IT-Arbeitsplätzen in den Fachbereichen (im Aufbau)

Mitarbeiterdaten der Hochschule werden von HIS-SVA übertragen und verwalten über diesen HS Account:

- E-Mailkonto der HS Lausitz (Microsoft Exchange Server)
- WLAN-Zugang an der Hochschule Lausitz
- Reisekostenverwaltung Reiko (PTravel Web)
- HTML-Webspace
- Softwareservice des HRZ (nur Administratoren)
- VPN-Zugang (für administrative Zwecke vorbehalten)

Weitere Dienste sollen für alle Hochschulangehörigen folgen.

Derzeit ist kein zusätzlicher Datenimport in die zentrale Benutzerdatenbank geplant. Auch die vorhandene und durch diese Datenbank gefüllte Active Directory Domain ist für den Aufbau einer hochschulweiten Domain nicht vorgesehen. Sie wird nur für den Microsoft Exchange Server (Groupware- und Nachrichtensystem) verwendet, über welchen der E-Maildienst angeboten wird.

3.1.2 In der Hochschulbibliothek (HB)

Seit 1996 werden in der Hochschulbibliothek Buch- und Nutzerdaten gemeinsam elektronisch verwaltet, um den Status eines Buches direkt mit den Nutzern in Verbindung zu bringen. Seitdem besteht eine nahezu manuelle Aufnahme der gesamten Nutzerdaten. Erst in den letzten Jahren ist es durch neue Softwareversionen und deren Anpassung gelungen, die Datenaufnahme von neu

immatrikulierten Studenten zu vereinfachen. Dazu wird ein SQL-Daten Export aus dem HRZ und ein Import in den Fremddatenpol des Bibliothekssystem (OCLC SunRise 3.7pl1) zu Semesterbeginn durchgeführt. Dieser Import der Daten wird zu festgelegten Terminen von Hand durchgeführt. Bei einer Neuanmeldung eines Studenten wird die Matrikelnummer als eindeutige Identifizierung herangezogen und der komplett gelieferte Datensatz aus dem Fremdnutzerpool geladen. So entfällt die umständliche Aufnahme von Adresse, Telefonnummer usw. Diese Nutzerdaten werden aber zur Kontrolle noch einmal abgefragt. Sie sind für den Ausleihbetrieb von enormer Bedeutung.

Der Bibliotheksnutzer bekommt eine Benutzernummer zugewiesen und bestätigt die Benutzungsordnung der Hochschulbibliothek mit seiner Unterschrift auf dem Bibliotheksausweis. Mit dieser Benutzernummer werden alle Ausleihvorgänge abgewickelt. Der Nutzer kann mit dieser Nummer den erweiterten OPAC nutzen, um z.B. entliehene Bücher vorzumerken, Bücher vom jeweils anderen Standort zu bestellen, Merklisten zu erstellen und persönliche Einstellungen im InfoGuide zu speichern.

Ein weiterer Abgleich von Nutzerdaten findet nicht statt. Die BibliotheksmitarbeiterInnen sind angehalten, den Nutzer regelmäßig nach Veränderungen der Kontaktdaten zu fragen, so dass die Nutzerdaten auf einem relativ aktuellen Stand gehalten werden.

3.1.3 In ausgewählten Studiengängen

Derzeit bietet das Hochschulrechenzentrum jedem Bereichsadministrator an, zu Semesterbeginn einen Datenabzug aus der zentralen Nutzerverwaltung per Email speziell für den angeforderten Bereich zu erhalten. Diese Daten beinhalten jedoch nur den Namen, Vornamen, das Login und werden manuell oder durch ein gestartetes Script in den vorhandenen lokalen Verzeichnisdienst eingetragen. Die Passwortvergabe erfolgt dezentral. Es findet kein automatischer Nutzerdatenabgleich statt.

Selbst in den einzelnen Fachbereichen und den einzelnen Studiengängen gibt es keine einheitliche Verwaltung. Teilweise hat jeder PC-Pool eine eigene Nutzerverwaltung. Im Studiengang Informatik existieren derzeit (Sommersemester 2010) 3 parallele und unabhängige Verzeichnisdienste, die die Authentifizierung in 6 PC-Pools übernehmen. Alle Änderungen und Gastzugänge werden per Hand eingetragen.

Im Sommersemester 2010 wurde den Administratoren ein von einem Studenten entwickeltes Softwareprogramm SQL2AD[16] vorgestellt, welches dazu verwendet werden kann, direkt Daten aus der zentralen SQL-Nutzerverwaltung in ein Active Directory System (ADS) einzupflegen und so das zentrale Login auch an den Arbeitsplätzen in den Fachbereichen anzubieten. Einzelne Fachbereiche bekundeten großes Interesse – zögern aber noch, da es keinerlei Erfahrungen in der Hochschule mit diesem Tool gibt. Im Kapitel 6.2.3 wird näher darauf eingegangen.

3.2 Zugang zu elektronischen Ressourcen

Ein Großteil der hauptsächlich von der Bibliothek erworbenen elektronischen Ressourcen werden über IP-Range Freischaltungen realisiert. Da alle Rechner innerhalb des HRZ- Netzwerkes, also im gesamten Campus, für einen Zugang zum Internet den Hochschul-Proxy www-cache.fh-lausitz.de:3128 einstellen müssen, gehen alle Rechner mit der Absender-IP-Adresse dieses Proxys nach außen. Jetzt kann ein Anbieter einer elektronischen Ressource den Zugang nur für diese IP-Adresse freigeben und jeder Rechner im Campusnetz hat freien Zugriff auf diese Quelle.

Diese Datenquellen sind auf der Internetseite der Hochschulbibliothek einzusehen und über den webOPAC recherchierbar. Da eine OPAC-Recherche auch von Rechnern außerhalb der Hochschule durchgeführt und z.B. E-Books als Treffer haben kann, ist die Anzeige zur Nutzung dieser Datenquelle für den Nutzer nicht eindeutig. Er muss erst in das Netz der Hochschule, um diese elektronische Ressource einsehen zu können – obwohl er Mitglied der Hochschule und / oder Bibliothek ist.

Es gibt derzeit keine Möglichkeit für Hochschulangehörige und externe Bibliotheksnutzer diese elektronischen Ressourcen von außerhalb der Hochschule zu nutzen, obwohl sie dazu berechtigt wären.

[16] [Seifert]

4 Anforderungen der Hochschulbibliothek an ein internes Identitätsmanagement

4.1 Authentifizierter Zugang zu den Arbeitsstationen in der Bibliothek

Wie bereits in Kapitel 2 beschrieben ist es im Moment gesetzlich nicht zwingend notwendig, eine Nutzerkontrolle für die Benutzung des Internets durchzuführen. Die Hochschulbibliothek strebt trotzdem an, nur registrierten Nutzern den Zugang zum Internet zu gestatten.

Begründung: Momentan hat jeder angemeldete Bibliotheksnutzer, aber auch jeder „Walk-in-User“ an den ca. 30 PC-Arbeitsplätzen freien Netzzugang. Somit kann dieser unkontrolliert missbraucht werden. Um dies zu verhindern, soll zukünftig eine Authentifizierung ermöglichen, nur noch angemeldeten Bibliotheksnutzern den Zugang zu gewähren. Wurde bisher ein Missbrauch dieser frei zugänglichen Plätze im HRZ festgestellt, war eine zeitlich begrenzte Netzwerkabschaltung der betroffenen Arbeitsplätze das einzige, aber nicht wirksame Mittel zur Unterbindung.

Eine weitere Anforderung der Hochschulbibliothek besteht in der Deaktivierung des Zugangs für Nutzer bei wiederholten Missbräuchen sowie bei Ablauf des Nutzerausweises. Sonstige Einschränkungen sind derzeit nicht geplant und sind laut DINI[17] auch nicht wünschenswert, damit der freie Zugang zu Informationen in einer öffentlich zugänglichen Hochschulbibliothek gewährleistet bleibt.

Ferner sind die PC-Arbeitsplätze der Hochschulbibliothek für Studienanfänger die nahezu einzigen frei zugänglichen Plätze, um sich im Hochschulnetzwerk registrieren zu können. Diese Registrierung ist Voraussetzung für viele Dienste der Hochschule. Daraus resultiert die dritte Anforderung. Der Zugang zu den Internetarbeitsplätzen muss schon kurz nach der Anmeldung in der Hochschulbibliothek möglich sein. Somit kann zu Semesterbeginn der Service für die Campusnetz-Authentifizierung weiterhin adäquat durch die Hochschulbibliothek angeboten werden.

Die Umsetzung dieses Projektes soll gleichfalls als Vorarbeit für die zu erwartenden neuen rechtlichen Restriktionen und Nachweispflichten dienen. Im gegebenen Fall sind dann nur noch kleine Anpassungen durchzuführen.

[17] [DINI ÖA]

4.2 Authentifizierter Zugang zu elektronischen Ressourcen der Hochschulbibliothek

Wie im Kapitel 3.2 beschrieben, ist derzeit außerhalb des Hochschulgeländes nur eine Recherche im OPAC der Hochschulbibliothek möglich. Die Nutzung der erworbenen Online-Ressourcen, wie E-Books, E-Journals und Datenbanken, kann momentan nur von den Rechnern auf dem Campus erfolgen.

Um den Bibliotheksnutzern ein flexibles Arbeiten auch außerhalb der Öffnungszeiten zu ermöglichen, muss es künftig einen zentralen authentifizierten Zugang geben, über den alle elektronischen Ressourcen zugänglich sind - sowohl vom Campus als auch von außerhalb unter Berücksichtigung der Lizenzbedingungen der Anbieter.

Als Mindestanforderung wird eine Authentifizierung gegen die Bibliotheksnutzerdatenbank gesetzt. Gleichzeitig soll eine genaue statistische Erhebung zur Nutzung der Online-Medien erstellt werden können, um:

1. auf Nutzerverhalten reagieren zu können und eventuell die Auswahl der elektronischen Ressourcen anzupassen
2. gegenüber der Hochschulleitung aussagekräftig zu sein, wie die ausgegebenen Mittel „verwertet“ wurden
3. die jährlichen Bibliotheksstatistiken BIX und DBS besser bedienen zu können und um nicht auf die sehr differenten Statistiken der Datenbankbetreiber angewiesen zu sein

Erweitert werden könnte die Anmeldung an den Arbeitsstationen und der Zugang zu den elektronischen Ressourcen durch eine Authentifizierung gegen die Zentrale Nutzerdatenbank. Somit könnten Hochschulangehörige auch mit dem zentralen Login einen Zugang bekommen und es würde für die Studenten einen weiteren Dienst mit nur einer Kennung geben.

4.3 Aktualität der Bibliotheksnutzerkonten

Studentendaten werden momentan an der Hochschule an mehreren Stellen verwaltet und sind nur schwer aktuell zu halten. Gerade mit Beginn jedes Semesters müssen bis zu 800 neue Studenten auch in der Hochschulbibliothek angemeldet werden.

Derzeit werden in regelmäßigen Abständen vor einem neuen Semester Datenbankexporte im HRZ erstellt und in der Hochschulbibliothek in einem sogenannten Fremddatenpool gespeichert. Diese Daten werden abgerufen, sobald sich ein neuer Student mit seiner Matrikelnummer in der Hochschulbibliothek anmelden will. Diese gesonderte Anmeldung ist notwendig, da die Erstbenutzer mittels Unterschrift auf dem Bibliotheksausweis nachweislich die Benutzungsordnung der Hochschulbibliothek akzeptieren müssen.

Mindestens dieser beschriebene Abgleich von Studentendaten soll automatisiert erfolgen. Wünschenswert wäre ein dynamischer Abgleich aller Daten von Hochschulmitgliedern mindestens unidirektional, so dass Adressdatenänderungen nur im Studentensekretariat durchgeführt werden und der Hochschulbibliothek für ein evtl. Mahnverfahren immer aktuelle Adressdaten zur Verfügung stehen.

Problem: Die Öffnungszeiten des Studentensekretariats sind weitaus geringer als die der Hochschulbibliothek. Daraus folgt, dass die Hochschulbibliothek zu großen Teilen über aktuellere Nutzerdaten verfügt. Deshalb wäre eine umgekehrte Aktualisierung der Nutzerdaten im Rechenzentrum, durch die Daten der Hochschulbibliothek von Vorteil. Wenn dies durch technische, rechtliche oder arbeitsorganisatorische Gründe nicht durchsetzbar ist, wäre ein Eintrag im Notizbuch wünschenswert.

4.4 Übersicht

Die Anforderungen lassen sich wie folgt zusammenfassen:

1.) Aktualität von Benutzerdaten

2.) Sammeln von Nutzerdaten in einem Verzeichnisdienst

3.) Clientzugang an Arbeitsstationen der HB

4.) Zugang von außen zu den elektronischen Ressourcen

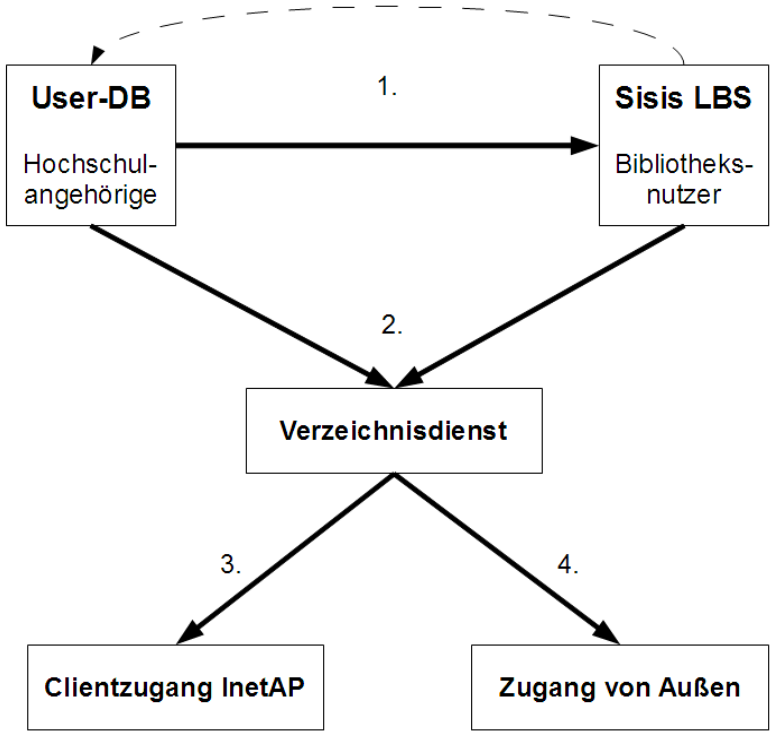

Abb. 3: Anforderungsübersicht

5 Ergebnisse einer Befragung zum Thema IDM in ausgewählten Hochschulen

5.1 Fragebogenanalyse

Um einen Einblick in die Handhabung des Identitätsmanagements innerhalb anderer Hochschulbibliotheken zu erhalten, wurde eine Befragung von vergleichbaren Einrichtungen durchgeführt. Für die Befragung wurde ein Online-Fragebogen erstellt (s. Anlage I), welcher sechs Schwerpunkte enthält. Diese lassen sich wiederum in drei große Themen unterteilen:

- Gibt es an der Hochschule ein Identitätsmanagement und wie ist es aus Sicht der Hochschulbibliothek organisiert?
- Bietet die Hochschulbibliothek den Zugang zum Internet an?
- Wie sind die elektronischen Ressourcen in die vorhandene IT-Struktur eingebunden?

Die Auswahl der befragten Hochschulbibliotheken erfolgte aus einer Übersicht[18] von ca. 200 Hochschulinternetseiten. Über die jeweilige Webpräsenz wurde dann die E-Mail-Adresse eines Ansprechpartners ermittelt. So wurden ca. 80 Fachhochschulen aus allen Bundesländern angeschrieben und gebeten, binnen eines Monats den Fragebogen auszufüllen. Die Teilnahme lag mit 33 ausgefüllten Fragebögen bei ca. 40%.

5.2 Auswertung

5.2.1 Identitätsmanagement in den befragten Hochschulbibliotheken

An ca. 30% der Hochschulen kommt kein zentrales Identitätsmanagement zum Einsatz. 70% haben ein zentrales Identitätsmanagement und dort wiederum ist bei 70% die Hochschulbibliothek in das hochschulinterne Identitätsmanagement integriert.

[18] [iFQ2010]

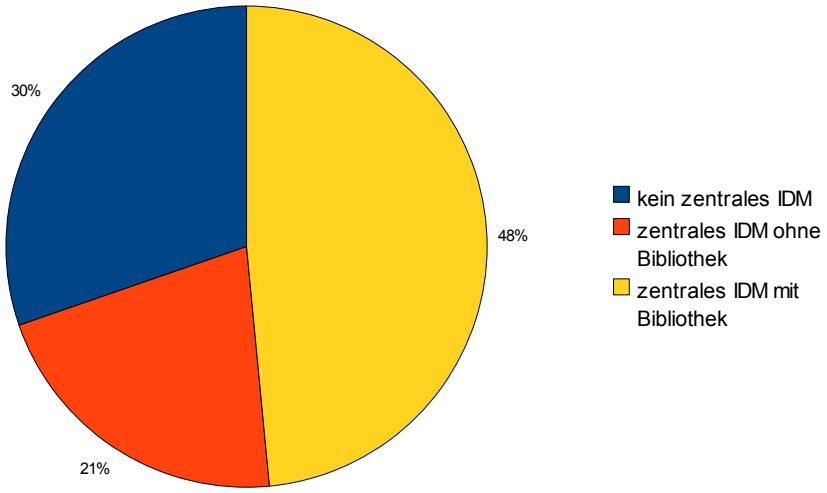

Abb. 4: Identitätsmanagement an Hochschule

Unabhängig vom zentralen Identitätsmanagement gibt es an ca. 30% der Hochschulen ein bibliothekseigenes Identitätsmanagement. In diesen Hochschulbibliotheken findet der Bibliotheks-Account zur Authentifizierung an den Internetplätzen Verwendung.

Bei ca. 30% der Hochschulen ist das Bibliothekspersonal in den Prozess der zentralen und bibliotheksinternen Nutzerverwaltung eingebunden. Dabei liegt die Federführung meist im Rechenzentrum.

5.2.2 Zugang zum Internet innerhalb der befragten Hochschulbibliotheken

Alle Hochschulbibliotheken bieten Ihren Nutzern Internetarbeitsplätze an.

Im Durchschnitt steht ein Internetarbeitsplatz ca. 250 Bibliotheksnutzern zur Verfügung, dabei schwankt die Quote von 100 bis knapp 4.000 Nutzer je Arbeitsstation. Man müsste für konkretere Aussagen das Nutzerverhalten genauer analysieren. Für den überwiegenden Teil der Hochschulen wird eine rege WLAN-Nutzung sowie das Angebot anderer öffentlicher Arbeitsplätze angenommen, so dass die Anzahl der bibliothekseigenen Arbeitsstationen durchaus ausreichend sein kann. Sicher spielt auch das angebotene Studienprofil eine große Rolle.

Eventuell handelt es sich auch um eine Hochschule, welche moderne digitale Medien unterdurchschnittlich nutzt.

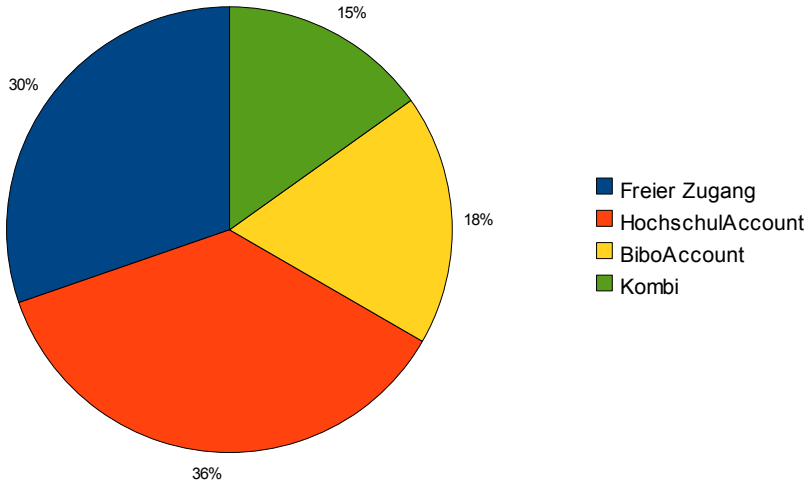

Abb. 5: Zugang zu Internetplätzen

Der Zugang erfolgt (siehe Diagramm) in 30% ohne Authentifizierung, in 70% nur über eine Authentifizierung. In diesen 70% spielt der Hochschulaccount mit 36% eine große Rolle, 18% geben nur den Bibliotheksnutzern einen Zugang – 15% stellen beide Authentifizierungsmöglichkeiten zur Verfügung.

5.2.3 Zugang zu Elektronischen Ressourcen

Alle Hochschulbibliotheken bieten ihren Nutzer elektronische Ressourcen zur Nutzung an.

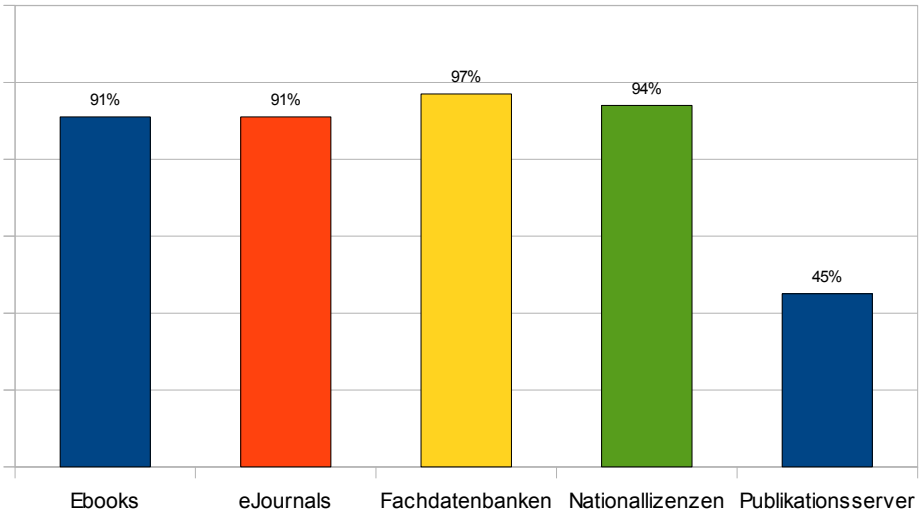

Abb. 6: Angebotene elektronische Ressourcen

Mehr als 90% aller Hochschulen versorgen die Nutzer mit elektronischen Ressourcen wie E-Books, E-Journals, Fachdatenbanken und Nationallizenzen. Ca. 45% bieten Ihren Nutzern auch den Zugang zu einem Publikationsserver.

Der Zugang zu diesen Ressourcen erfolgt im überwiegenden Maße frei im Campus/Bibliotheksnetzwerk. Nur ca. 15% regeln den Zugang über eine Authentifizierung auch innerhalb der Hochschule.

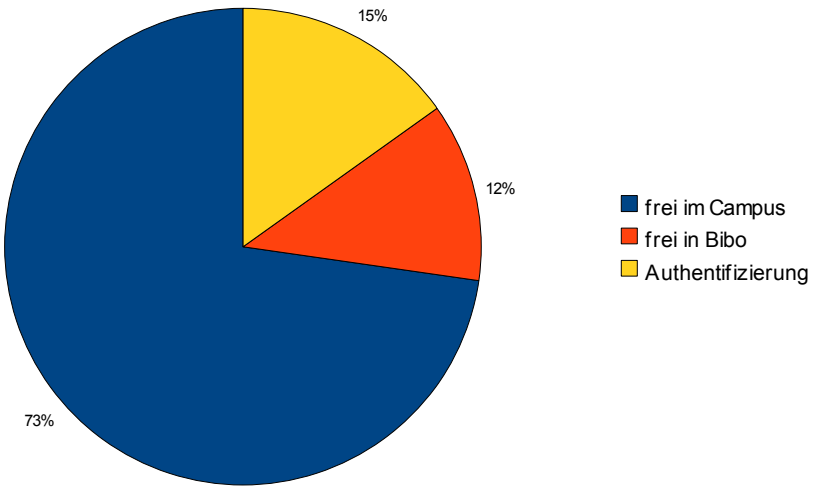

Abb. 7: Zugang zu elektronischen Ressourcen

Ca. 80% der HS bieten ihren Nutzern für die erworbenen Zugänge zu elektronischen Ressourcen auch den Zugriff von außen an. Diese HS realisieren diesen Zugang zu nahezu 90% über eine VPN-Verbindung. Dabei steht diese Möglichkeit nur Hochschulmitgliedern zur Verfügung, externe Nutzer haben keinen Zugriff auf diese Dienstleistung.

Ca. 18% bieten den Zugang mit Shibboleth an oder erarbeiten einen Zugang.

5.3 Schlussfolgerung

Im Vergleich zu den Hochschulen, die geantwortet haben, befindet sich die Hochschulbibliothek der HL im IDM-Service im unteren Mittelfeld. Die HL verfügt über ein zentrales IDM, in welches die Hochschulbibliothek derzeit nicht eingebunden ist. Die Hochschulbibliothek verfügt über ca. 35 Computerarbeitsplätze mit freiem Zugang zum Internet. Campusweit sind eine Vielzahl von elektronischen Ressourcen verfügbar. Ein Zugriff von extern ist jedoch nicht möglich.

Dies spiegelt die Forderungen der Hochschulbibliothek an ein Identitätsmanagement (s. Kapitel 4) deutlich wieder:

1. Aktualität der Nutzerdaten
2. authentifizierter Zugang zum Internet
3. Zugang zu elektrischen Ressourcen von außerhalb der Hochschule.

6 Mögliche Lösungsvarianten

6.1 Aktualität der Bibliotheksnutzerkonten

Wie bereits beschrieben, werden derzeit an der HL Nutzerdaten mehrfach verwaltet. Das führt vor allem in der Hochschulbibliothek zu einem erhöhten Arbeitsaufwand. Diese Problematik wurde bereits an vielen Hochschulen betrachtet und teilweise optimiert. Da solche Lösungen durch sehr unterschiedliche IT-Infrastrukturen, Personal- und Finanzmittel nicht 1:1 übernommen werden können, gilt es ,die Lösungsvarianten zu analysieren.

Dabei muss vor allem das eingesetzte LBS analysiert werden, da dieses die Daten vorhält und nur eine geringe Anzahl von Schnittstellen zur Verfügung stellt. So bietet das an der Hochschule Lausitz eingesetzte SunRise - Bibliothekssystem von OCLC nur eine Möglichkeit, Daten im System zur Verfügung zu stellen - einen Datenimport über einen sogenannten Fremddatenpool.

Alle weiteren Daten Im-/Exporte müssten direkt über die SQL-Datenbank laufen, was immer eine Analyse und die Erstellung von Konsistenschecks nach sich zieht. Die allgemeinen Nutzerdaten sind auf 11 Tabellen in der SQL-Datenbank verteilt.

6.1.1 Datenabgleich mit Scripting

Für den Datenimport bietet das LBS einen sogenannten Fremddatenpool an. Werden neue Nutzer angemeldet werden, können vorhandene Daten angezeigt und übernommen werden. Dann wird der Inhalt automatisch in die entsprechenden Tabellen verteilt. Dieser Pool wird momentan immer zu Semesterbeginn mit den neuen Studentendaten gefüllt, alte Einträge werden vorher gelöscht. Dazu diente das systemeigene Programm SIBUFP, das über die Administration angesprochen werden kann (Jahresarbeiten → Benutzerdatenupdate). Da dies mehrere manuelle Einsätze erfordert, könnte es durch einen automatischen Datenexport aus dem Rechenzentrum, mit anschließenden Datentransfer zum LBS und einem automatischen Import in das LBS ersetzt werden. Mit diesen importierten Nutzerdaten könnten auch dynamisch weitere Änderungen in Tabellen des LBS durchgeführt werden.

Für den Datenexport aus dem LBS könnte eine ähnliche Vorgehensweise mit dem HRZ vereinbart werden.

Viele Hochschulen setzen diesen Datenabgleich in Form von Skripten ein, um zentral vorliegende Studentendaten im Fremddatenpool des LBS zu speichern. Somit können auch externe Nutzer und Gastnutzer aus dem Bibliothekssystem exportiert werden, um für diese Nutzergruppen keine doppelte Erfassung durchzuführen.

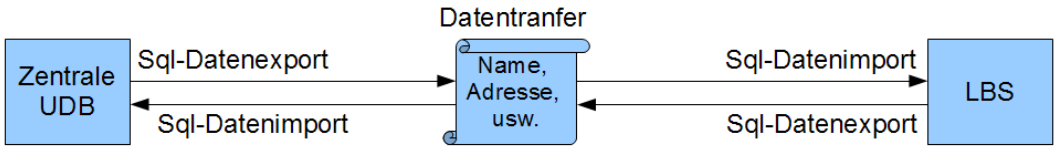

Abb. 8: Datenabgleich mit Skripting

Vorteile:

- keine zusätzlichen Kosten
- schnell umsetzbar

Nachteile:

- zeitkritischer Datenabgleich

6.1.2 Datenabgleich mit Identity Management Connector (OCLC)

Der IDM-Connector von OCLC stellt ein kommerzielles Produkt dar, welches für den Austausch von Benutzerdaten zwischen unterschiedlichen IDM-Systemen entwickelt wurde. Ein Hauptaugenmerk wurde auf die Integration der OCLC-eigenen Bibliotheksverwaltungsysteme Pica und SunRise gelegt. Somit ist die Verwaltung des IDM-Connectors in der administrativen Umgebung von SunRise eingebunden. Dabei werden LDAP fähige Verzeichnisdienste unterstützt.

Der IDM-Connector besteht aus folgenden Komponenten:

- Reader und Writer
  Der Datenaustausch mit den Targets läuft über jeweils individuell konfigurierbare Schnittstellen – dabei nimmt der „Reader“ die von einem Quellsystem gelieferten Daten entgegen, der „Writer“ übernimmt die Ausgabe an ein Zielsystem.
- Task-Manager
  Der Task-Manager übernimmt die Steuerung des Datenstroms vom Reader zum Writer.

- Administration
  Über die Administrationsoberfläche werden sämtliche Konfigurationen der einzelnen Komponenten verwaltet. Dazu stehen zahlreiche Parametrisierungsmöglichkeiten zur Verfügung.

- Authentifizierung
  Zusätzlich beinhaltet der IDM-Connector eine Authentifizierungskomponente, den Identity Server (IDS) – damit wird eine Schnittstelle zur Prüfung von Benutzerkennungen und Passwörtern angeboten.

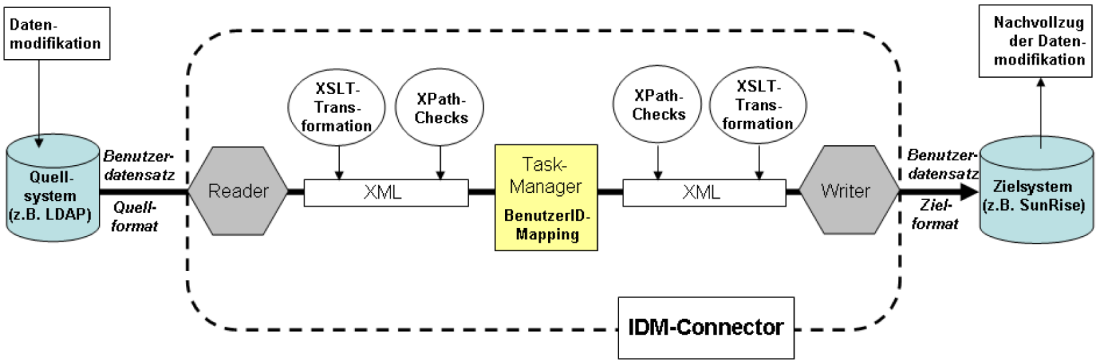

Abb. 9: Benutzerdatensynchronisation (unidirektional) mit OCLC IDM-Connector
Quelle: [IDM-C] Seite 10

Die Verarbeitung von Benutzerdaten kann kurz in fünf Schritten erklärt werden:[19]

1. Quelltarget übergibt die Daten an die Schnittstelle des Readers
2. Daten werden in ein definiertes XML-Format umgewandelt
3. Prüfung der Daten durch den Task Manager und Weiterleiten an entsprechenden Writer
4. Daten werden wieder in ein definiertes XML-Format überführt
5. Writer empfängt Daten und übergibt diese an das Zielsystem

z.B. könnte so ein LDAP-Server ausgelesen werden und die Daten in das LBS eingetragen werden. Das gleiche in die umgekehrte Richtung, um aktualisiere Nutzerdaten an das LDAP-Verzeichnis zu melden.

[19] [IDM-C] Seite 9

Vorkonfigurierte Reader/Writer:

- LDAP
- OpenLDAP
- SLNP (OCLC eigene Kommunikationsschnittstelle zu SunRise)
- LBS (OCLC eigene Kommunikationsschnittstelle zu Pica)
- XML
- sonstige (Schnittstelle für Eigenentwicklungen)

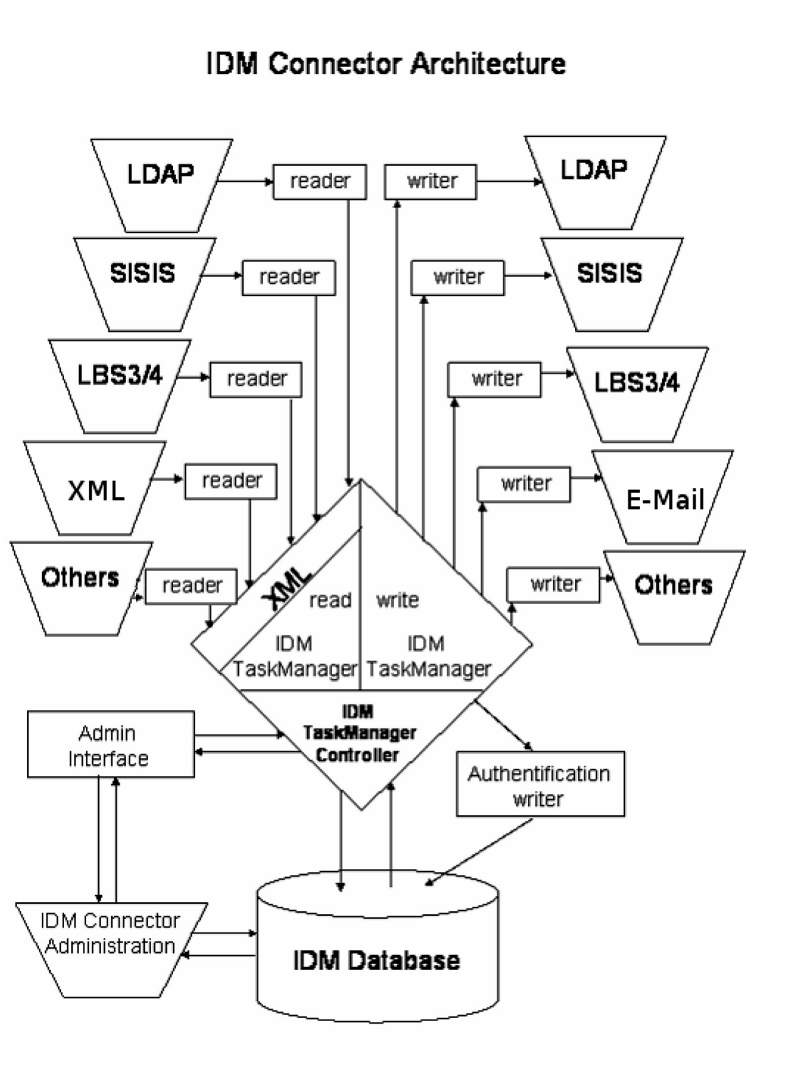

Abb. 10: Aufbau des OCLC IDM-Connector
Quelle: [IDM-C] Seite 13

Vorteile:

- vielseitige Erfahrungen an unterschiedlichsten Hochschulen
- mächtiges und sehr variables System

Nachteile:

- komplexe Verwaltung
- keine Targetschnittstelle zu einer SQL-Datenbank → Entwicklungsaufwand

6.2 Verzeichnisdienst

Ein Verzeichnis ist eine Sammlung von gleichwertigen Informationen. Telefonbücher, Speisekarten, Versandkataloge können als Verzeichnisse angesehen werden, dabei liegt allen Verzeichnissen ein ordnendes Prinzip zu Grunde.[20]

Ein Verzeichnisdienst ist eine „Zentrale, einheitliche Datenbank über sämtliche menschlichen und maschinellen Ressourcen einer vernetzten Arbeitsumgebung sowie von Metadaten der ganzen IT einer Unternehmung: Namen, Adressen, Telefonnummern, Geräteparameter, Zugriffsrechte, Datenbeschreibungen, Spezifikationen, Routing-Informationen usw.“.[21] Dabei organisiert ein Verzeichnis seine Daten in Form einer baumartigen Hierarchie, dem sogenannten Verzeichnisbaum.

Jegliche Authentifizierung und Nutzerverwaltung erfordert einen Pool von berechtigten Nutzern. Leider existiert derzeit kein für die Hochschulbibliothek erreichbarer Pool, der die folgenden Bedingungen erfüllt:

- alle berechtigten Bibliotheksnutzer (mit Benutzernummer und OpacID)
- alle berechtigten HS Nutzer (mit zentralem Login und Bibliotheksaccount)

Somit steht als erstes der Aufbau eines solchen Nutzerpools, also eines Verzeichnisdienstes an.

Zur Verwaltung von Nutzerdaten und Berechtigungen haben sich in den letzten Jahren LDAP-basierende Verzeichnisdienste durchgesetzt.

Das LDAP (Lightweight Directory Access Protocol) entstand Anfang der 90er Jahre aus dem Standard X.500 der International Telecommunication Union (ITU) aus dem

[20] [Geier]
[21] [Fisch] S. 900

Jahr 1988 für den Aufbau eines globalen Verzeichnisdienstes. Die X.500 definiert zwei Subprotokolle, zum einen DAP (Directory Access Protocol) das die Client - Server - Kommunikation regelt und die DSP (Directory Service Protocol), welche die Kommunikation zwischen den Servern beschreibt.[22]

LDAP entwickelte sich dabei zu einem offenen und weltweit eingesetzten Standard für die Kommunikation mit einem Verzeichnisdienst. Der ursprüngliche Standard X.500 stellte lange Zeit eine Referenz für Verzeichnisdienste dar. LDAP ist dabei weniger komplex und beherrscht die Kommunikation auf TCP/IP-Basis.[23]

Hinter LDAP verbirgt sich also die reine Kommunikation zwischen einem Clienten- und einem Verzeichnisdienst-Server. Diese Kommunikation findet im sogenannten Frontend statt. Im Backend erfolgt die Verarbeitung dieser Daten. Das Backend lässt sich in drei unterschiedliche Bereiche aufteilen[24]:

1. Lesen/Schreiben aus/in eine Datenbank, hier könnten neben hierarchischen auch relationale Datenbanken angesprochen werden.
2. Zwischenspeichern z.B. in einem LDAP-Proxy
3. Generieren von Daten zur Laufzeit, z.B. Monitoring oder externe Programmaufrufe

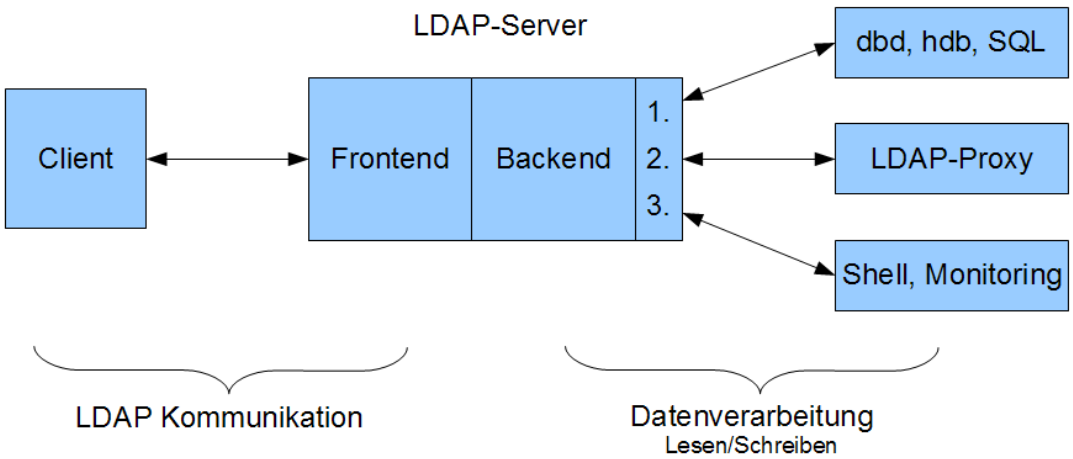

Abb. 11: Ablauf der LDAP Kommunikation

[22] [Klünter]
[23] [Huber]
[24] [Liebel] S. 31

Damit ein LDAP-Server Nutzerdaten speichern kann, wird mit dessen Backend eine Datenbankverbindung aufgebaut. In den meisten Fällen handelt es sich um eine hierarchische Datenbank, da sich ein Verzeichnisbaum auch hierarchisch aufbaut. Als Standard hat sich hierbei die Berkeley Database etabliert.

Auf Grund dieser variablen Backends ergeben sich zwei grundlegende Möglichkeiten (siehe Abbildung 12):

1. der Datenexport aus einer SQL-Datenbank und der anschließende Import mit Hilfe des LDAP-Protokolls in eine separate LDAP-Datenbank
2. Kommunikation über ein LDAP-Backend direkt mit der existierenden Datenbank.

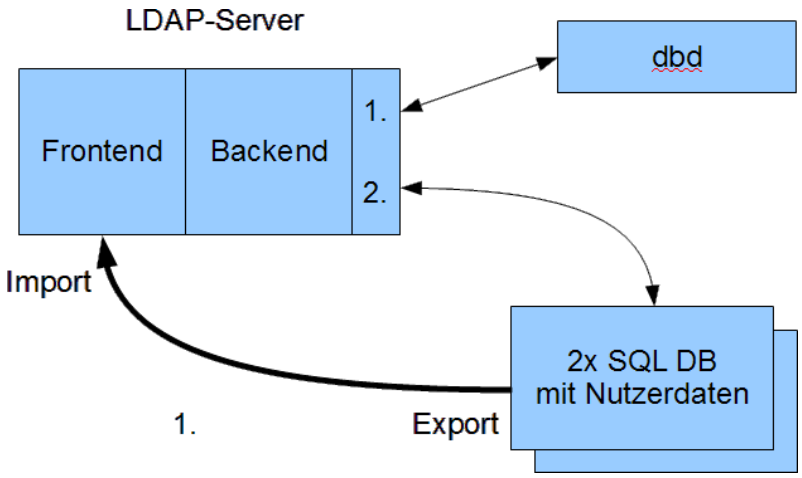

Abb. 12: Schema des LDAP-Datenimports

6.2.1 Datenübernahme per Scripting

In allen LDAP Versionen wird ein Datenimport per Scripting angeboten. Dabei gibt es Shell-Kommandos für das Hinzufügen (ldapadd), Löschen (ldapdelete) und Verändern (ldapmodify) von Einträgen im LDAP-Baum. Für diese Manipulationen stehen auch eine Vielzahl von LDAP-Modulen für die gängigsten Programmiersprachen (z.B. PHP[25] und Java[26]) zur Verfügung. Somit könnten alle auf LDAP-basierenden Verzeichnisdienste mit Hilfe von Exportdateien oder direktem Zugriff auf die Datenbanken (z.B. per ODBC oder JDBC) gefüllt werden .

[25] [PHP]
[26] [Java]

Die einfachste Methode der vollständigen Migration von Daten stellt die Überführung der Daten in das textbasierte LDAP Data Interchange Format (LDIF) dar.[27]

Nachteil:

- manuelles Entladen und Transferieren von Exportdateien
- Programmieraufwand mit umfangreicher Fehleranalyse und Tests

Vorteil:

- keine zusätzlichen Kosten
- mit freier Software realisierbar

6.2.2 Datenübernahme mit Identity Management Connector (OCLC)

Wie in Kapitel 6.1.2 beschrieben, lassen sich mit dem IDM Connector von OCLC Daten abgleichen und so auch Verzeichnisse aufbauen.

Es existiert eine SLNP-Schnittstelle zum Auslesen von Daten aus dem LBS, jedoch keine, um direkt aus einer SQL-Datenbank Daten auszulesen. Damit besteht die Notwendigkeit, eine solche Schnittstelle mit hohem Aufwand zu implementieren. Möglich wäre auch ein LDAP-Verzeichnis, das die benötigten Daten enthält und mit der SQL-Datenbank abgleicht. Das wiederum benötigt eine SQL-LDAP-Schnittstelle, aber mit einem OpenLDAP-Postgres-Backend realisierbar wäre.

[27] [Schoen] S.18

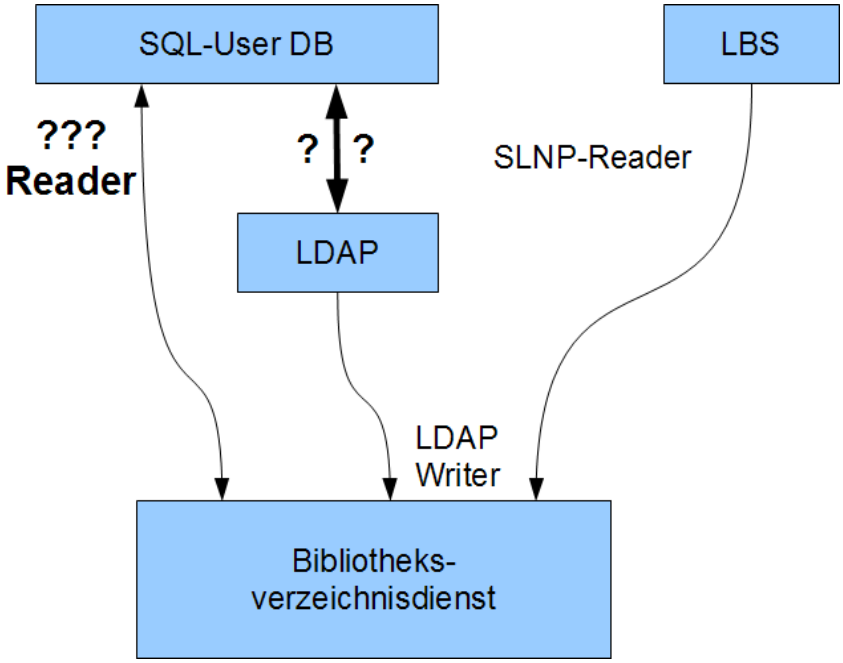

Abb. 13: Schema des IDMC-Datenimports

Nachteil:

- hoher Entwicklungsaufwand

6.2.3 Datenübernahme mit SQL2AD[28]

Dies ist eine speziell für die Hochschule Lausitz (FH) entwickelte Software zur Datenreplikation zwischen SQL-Datenbanken und einem Active Directory Service. Als exemplarische Datenbank wurde die zentrale Nutzerdatenbank der Hochschule herangezogen.

Diese Software ist dabei variabel konfigurierbar, so dass jegliche Art von SQL-Datenbanken mit geeignetem Dateninhalt ausgelesen werden kann, um daraus Nutzerdaten in ein Active Directory zu überführen. Die Kommunikation läuft über eine JDBC-Schnittstelle. Mit dieser ist jeder SQL-Datenbanktyp auslesbar.

So könnte mit diesem Tool die Datenbank des LBS und die zentrale Nutzerdatenbank ausgelesen, beide in einem ADS zusammengefasst und so der geforderte Pool von Nutzerdaten in einem AD-Verzeichnisdienst bereitgestellt werden.

[28] [Seifert]

Vorteil:

- für die Hochschule frei zugängliche Software
- für den internen Gebrauch entwickelt und teilweise exemplarische Lösungen vorhanden
- Großes Administratoreninteresse und damit Erfahrungen vorhanden

Nachteil:

- gebunden an ein Active Directory, nur mit Aufwand auch für andere LDAP Verzeichnisse nutzbar

6.2.4 Alternative OpenLDAP mit SQL-Backend

Alternativ zum Füllen einer separaten LDAP-Datenbank, könnte ein LDAP-Server mit angeschlossenen SQL-Backend sein. Somit werden die Nutzerdaten nicht direkt in der LDAP-Datenbank abgefragt, sondern in der über das angeschlossene und konfigurierte SQL-Backend[29] direkt in der SQL-Datenbank ausgelesen.

Nun wäre es möglich, beide SQL Datenbanken direkt in die Verzeichnisstruktur mit Hilfe eines SQL- Backends einzubinden. Hierzu müsste allerdings der Umweg über eine höhere Programmiersprache gewählt werden. Grund dafür sind die Datenbankzugangsschnittstellen wie ODBC oder JDBC. Diese können genutzt werden, da kein direkter Zugriff auf die Datenbanken vorhanden ist. Derzeit existieren nur für MySQL und PostgreSQL direkte SQL-Backends für einen OpenLDAP-Server.

Vorteil:

- direkter Zugriff auf die Nutzerdaten aus Datenbank (kein Zwischenspeichern)
- sofort verfügbar (Änderungen in der Datenbank, sind sofort im LDAP-Verzeichnis abrufbar)

Nachteile:

- nur mit OpenLDAP realisierbar
- Entwicklung notwendig

[29] [IM HS] S. 383f.

6.3 Authentifizierter Zugang zum Internet an Arbeitsstationen der Hochschulbibliothek

Bei der Authentifizierung gilt es, zwischen drei Zugangsmöglichkeiten zu unterscheiden

1) Keine Anmeldung an der Arbeitsstation, aber beim Zugang zum Internet – d.h. freie Nutzung der Arbeitsstationen z.B. Office-Produkte, Intranet und Druck, erst beim Zugang zum Internet Authentifizierung notwendig.

2) Anmeldung an den Arbeitsstationen, mit freiem Zugang zum Internet – d.h. jegliche Nutzung der Arbeitsstationen erfordert einmalige Autorisierung.

3) Kombination aus beiden – evtl. als Single-Sign-On-Lösung, d.h. erst Anmeldung an Arbeitsstationen und dann Autorisierung beim Zugang zum Internet.

6.3.1 Authentifizierung an Proxy beim Zugang zum Internet

6.3.1.1 WebControl OCLC

WebControl ist ein kommerzielles Produkt der Firma OCLC. Es stellt eine Zusatzkomponente zum bestehenden Bibliotheksverwaltungssystem SunRise dar und ermöglicht die zeitliche und inhaltliche Kontrolle von Nutzern beim Zugang zum Internet. Somit können Nutzern je nach Nutzergruppe oder einzeln verschiedene Berechtigungen und Kosten zugewiesen werden.

WebControl bietet folgende Funktionalitäten:[30]

- Authentifizierung im Browser gegen LBS mit Nutzernummer und Opac-ID,
- maximale Dauer der Internet-Nutzung pro Tag konfigurierbar,
- Möglichkeit der Gebührenerhebung pro Zeitintervall der Internetnutzung mit automatischer Verbuchung im Benutzerkonto,
- kostenfreie Surfzeit pro Tag,
- Nutzerberechtigungen direkt über Ausleih-Client des LBS einstellbar.

Zur Verwaltung der Internetzugriffe wird ein separater Proxy-Server eingesetzt, es handelt es sich um Squid – einen freien Proxy-Server nach GNU General Public Licence.

[30] [SISISwC2005]

WebControl stellt also eine direkte Verbindung zwischen Proxy-Server und dem LBS her. Alle Zugänge zum Internet werden im Ausleih-Client und in der Systemadministration konfiguriert[31].

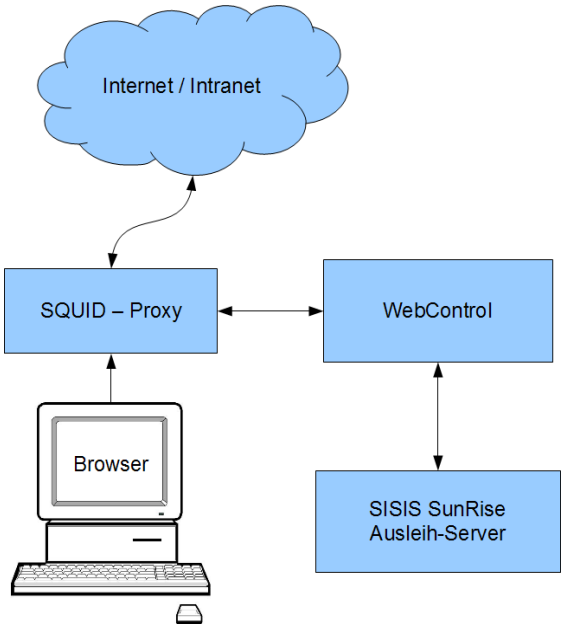

Abb. 14: Schema der Funktionsweise von WebControl

Vorteile dieser Lösung:

- ausgetestetes und leicht integrierbares Programmmodul
- alle Softwarekomponenten sind aufeinander abgestimmt

Nachteile dieser Lösung:

- Kosten
- nur Authentifizierungen gegen LBS über SLNP-Schnittstelle, keine anderen Authentifizierungsmöglichkeiten

6.3.1.2 Vorhandene Hochschul-Proxy-Authentifizierung

Es existiert eine Proxy-Authentifizierung an der Hochschule Lausitz, mit welcher alle Wohnheimanschlüsse nur nach erfolgreicher Authentifizierung, Zugang zum Internet erhalten. Diese Authentifizierung erfolgt indirekt gegen die zentrale Nutzerdatenbank. Da in dieser nur interne Hochschulangehörige eingebunden sind, wären die externen Nutzer der Hochschulbibliothek von der Nutzung ausgeschlossen.

[31] [FGMwC3.7]

Vorteile:

- kein weiterer Aufwand, Nutzung kann einfach übernommen werden

Nachteile:

- keine Möglichkeit der Zugangssteuerung für die Bibliothek
- externe Nutzer ausgeschlossen

6.3.1.3 Eigene Proxy-Authentifizierung

Mit dem vorhandenen Pool von berechtigten Nutzern wäre auch eine eigene Proxy-Authentifizierung möglich. Hierzu könnte ein eigener Hochschulbibliotheks-Proxy-Server eingerichtet werden, welcher an allen betreffenden Arbeitsstationen eingetragen wird und alle Anfragen authentifiziert und danach an den zentralen Hochschul-Proxy weiterreicht.

Dieser Proxy würde es auch ermöglichen, für Rechnerarbeitsplätze mit speziellen Aufgaben (z.B. PCs in Arbeitskabinen, Scan- und Multimediaarbeitsplätzen) eine Authentifizierung nur für den Zugang zum Internet durchzuführen.

6.3.2 Clientanmeldung

In der Hochschulbibliothek werden derzeit WindowsXP Rechner eingesetzt. Das von Microsoft verwendete Kommunikationsprotokoll SMB (Server Message Block) stellt die Basis der Netzwerkdienste von Windows-Betriebssystemen dar.

Neben dem Windows-Server unterstützt auch die frei verfügbare Software Samba dieses Protokoll.

Eine Windowsanmeldung ist auch mit Hilfe der freien Software pGina[32] möglich. Sie erlaubt es, eine Authentifizierung gegen unterschiedlichste Server (ua. LDAP, POP3, RADIUS, SSH uva.) durchzuführen. Durch dieses Tool lassen sich Windowsrechner auch gegen „Nicht-Windows-Server“ authentifizieren.

[32] Internet: http://www.pgina.org [18.11.2010]

6.4 Authentifizierter Zugang zu elektronischen Ressourcen

6.4.1 Shibboleth - DFN-AAI

Ausgehend vom Bundesministerium für Bildung und Forschung[33] geförderten AAR-Projekt[34], wurde in Deutschland in den letzten Jahren eine Infrastruktur zur Authentifizierung und Autorisierung (AAI) aufgebaut. Der DFN-Verein übernimmt in Deutschland die Koordination dieser Föderation von Anbietern und Nutzern elektronischer Ressourcen.[35]

Folgende Ziele werden mit dem Projekt verfolgt[36]

- ortsunabhängiger Zugriff auf lizenzierte elektronische Ressourcen,
- Nutzung aller von der Institution lizenzierten elektronischen Ressourcen nach einmaliger Anmeldung (Single Sign-On)
- einfache Anbindung an bestehende Identitätsmanagementsysteme (z.B. SQL, LDAP),
- Schutz lizenzpflichtiger elektronischer Ressourcen vor unberechtigtem Zugriff,
- keine eigene Benutzerverwaltung des Anbieters elektronischer Ressourcen,
- statistische Auswertung der Nutzungsdaten

Shibboleth stellt ein Verfahren zur verteilten Authentifizierung und Authorisierung für Internetdienste dar. Shibboleth sieht vor, dass sich der Benutzer nach einer Authentifizierung mit seiner lokalen Hochschulkennung ortsunabhängig auf von der Hochschule lizenzierte Inhalte verschiedener Anbieter zugreifen kann.

Dabei ist das Shibboleh-System aus drei Komponenten aufgebaut:

- Identity-Provider: befindet sich bei der Hochschule
- Service-Provider: befindet sich beim Anbieter
- Lokalisierungsdienst

---

33 Internet: http://www.bmbf.de/ [01.12.2010]
34 Internet: http://aar.vascoda.de/ [28.11.2010]
35 Internet: https://www.aai.dfn.de/ [29.10.2010]
36 [Borel]

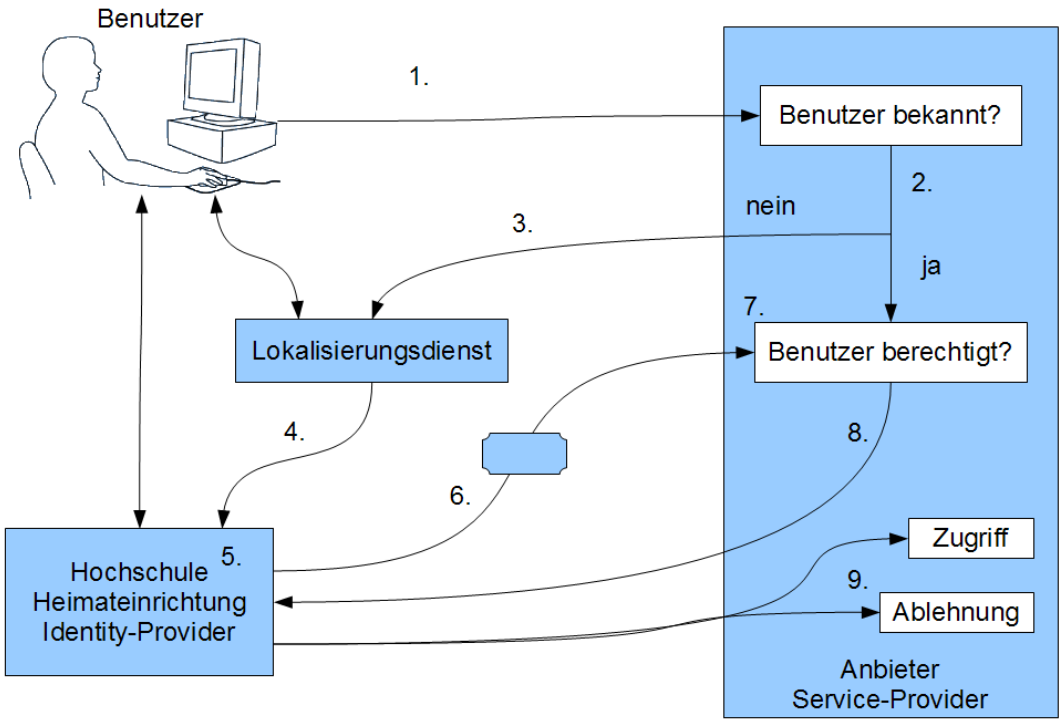

Abb. 15: Ablauf der Authorisierung mittels Shibboleth

Ablauf:

1. Ein Benutzer will auf eine geschützte elektronische Ressource eines Anbieters zugreifen.
2. Der Anbieter nimmt die Anfrage entgegen und überprüft, ob der Benutzer bereits authentifiziert ist.
3. Wenn nicht, wird er zum Lokalisierungsdienst weitergeleitet. Der Lokalisierungsdienst bietet eine Auswahl von Einrichtungen an.
4. Der Benutzer wählt seine Heimateinrichtung aus und wird zu dieser weitergeleitet.
5. Die Heimateinrichtung prüft, ob der Benutzer bereits authentifiziert ist. Ist dies nicht der Fall, wird der Benutzer aufgefordert, dies zu tun.
6. Die Heimateinrichtung stellt einen "digitalen Ausweis" aus und leitet den Benutzer zum Anbieter zurück.
7. Der Anbieter prüft den Inhalt dieses digitalen Ausweises.

8. Benötigt der Anbieter weitere Informationen, um zu entscheiden, ob der Benutzer auf die gewünschte Ressource zugreifen darf (zum Beispiel der Studiengang), so fragt er bei der Heimateinrichtung des Benutzers nach.

9. Der Anbieter prüft über das eigene System, ob der Benutzer auf die Ressource zugreifen darf, und gestattet den Zugriff oder lehnt ihn ab.

Die Anzahl der Dienste auf Basis von Shibboleth, sowie die Verbreitung und Akzeptanz nimmt stetig zu. Derzeit wird im KOBV ein Shibboleth-Projekt[37] umgesetzt, um die Online-Fernleihe, OPAC-Authentifizierung und den KOBV-Dokumentenserver (OPUS) über diesen Dienst anzubieten.

6.4.2 Rewrite Proxy z.B. HAN oder EZProxy

Bei EZProxy[38] bzw. HAN[39] handelt es sich jeweils um kommerzielle Software der Firmen OCLC bzw. H+H. Dahinter verbirgt sich ein sogenannter Rewrite-Proxy. Er erlaubt es, Benutzern auch außerhalb eines Campus-Netzwerkes Zugang zu Online-Ressourcen zu gewähren, auch wenn diese via IP mit der jeweiligen Netzadresse authentifiziert werden. Dazu werden in der Software spezielle URLs generiert, die jeweils einen Zugang z.B. zu einer Online-Datenbank repräsentieren. Der Benutzer ruft dann diese URL auf, muss sich am Rewrite-Proxy authentifizieren und wird dann zu dieser elektronischen Ressource weitergeleitet. Bei der Weiterleitung werden jedoch alle HTML-Seiten so umgewandelt, dass sämtliche Links vom Rewrite-Proxy umgeschrieben werden (daher Rewrite) und der Nutzer so immer wieder über diesen Zugang und somit mit der Absender-IP-Adresse der Bibliothek mit der Ressource kommuniziert.[40]

Vorteile:

- einfacher und unkomplizierter Zugang zu elektronischen Ressourcen[41]
- ortsunabhängiger Zugang auf die Bibliotheksangebote
- Authentifizierung gegen LBS oder Verzeichnisdienst
- statistische Auswertung der Nutzung

---

37 Internet: http://www.kobv.de/ueber_den_kobv/fe_projekte/bvb_kobv_projekte/rechtemanagement_mit_shibboleth/ [18.10.2010.]
38 [EZP]
39 [HAN]
40 [Gragert]
41 [UZH.CH]

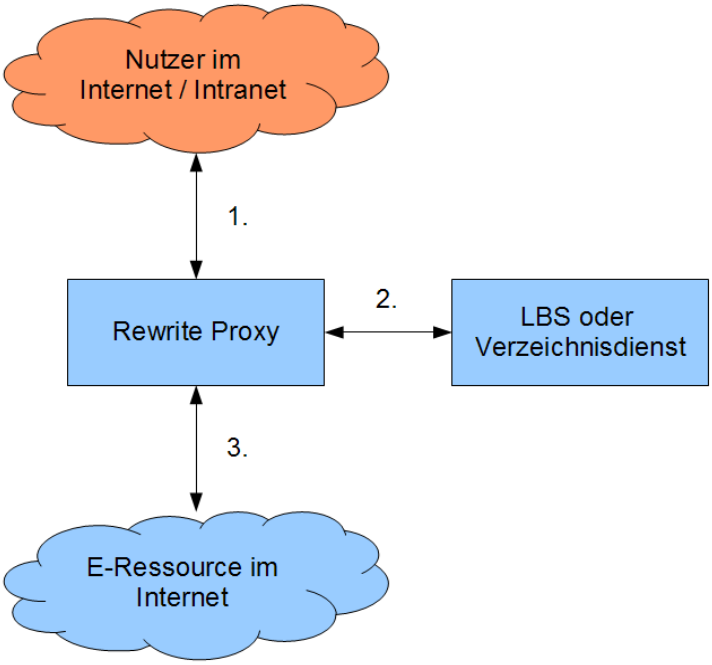

Abb. 16: Schematische Darstellung eines Rewrite-Proxy

Die Abbildung 16 stellt den Ablauf schematisch dar:

1. Nutzer aus dem Internet kommuniziert nur mit Rewrite-Proxy.
2. Er wird gegen Verzeichnisdienst oder LBS authentifiziert.
3. Bei Erfolg setzt sich der Rewrite-Proxy mit der elektronischer-Ressouce (E-Books, Datenbanken, etc.) in Verbindung.

Der Rewrite-Proxy stellt also eine Art Vermittler zwischen elektronischerRessource und Nutzer dar. Es besteht keine direkte Kommunikation zwischen beiden.

6.4.3 Virtuelle Private Netzwerke (VPN)

Ein VPN schließt Computer oder ganze Netzwerke über ein unsicheres Netz (z.B. Internet) virtuell an ein sonst abgeschlossenes Netzwerk (in diesem Fall Campusnetz) an. Das Netz bzw. der angeschlossene Computer werden so virtueller Bestandteil dieses Netzwerkes mit allen dort geltenden Nutzungsregeln (z.B. Proxyeinstellungen).

Die Datenübertragung durch eine VPN-Verbindung erfolgt in verschlüsselter Form durch das dazwischen liegende unsichere Netzwerk. Eine VPN-Verbindung wird immer zwischen einem VPN-Client und einem VPN-Server aufgebaut. Diese virtuelle Punkt-zu-Punkt Verbindung ist ähnlich einer direkten Kabelverbindung anzusehen.

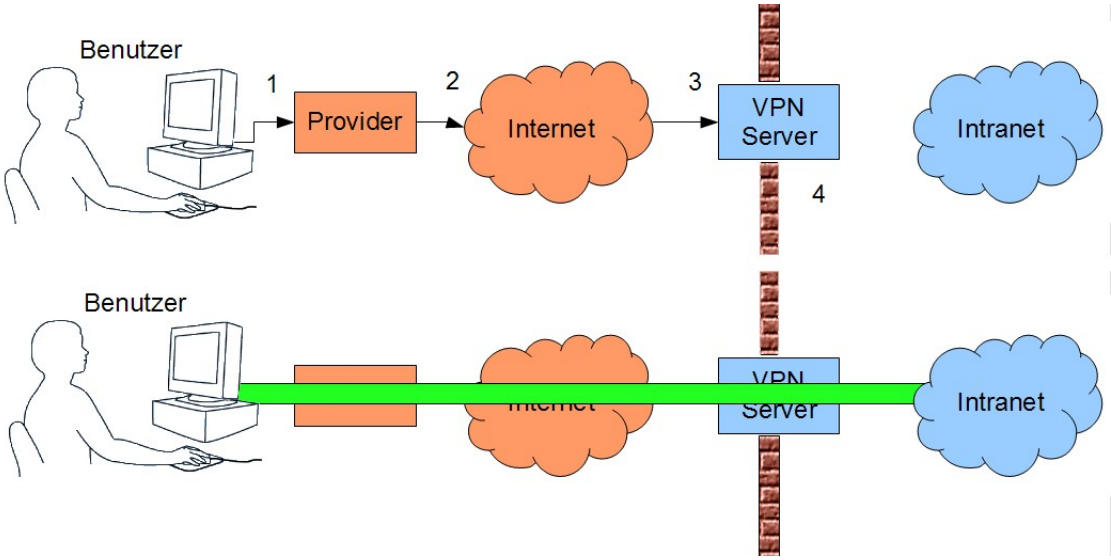

Abb. 17: Schematische Darstellung eines VPN-Tunnels

In der Abbildung 17 ist zu sehen:

1. Als erstes wird eine Verbindung zu einem beliebigen Provider vom VPN-Client hergestellt. Dazu kann jede verfügbare Zugangstechnik (z.B. DSL[42], HSCSD, UMTS[43] etc.) verwendet werden!
2. Dieser stellt die Verbindung zum Internet her.
3. Anschließend erfolgt der Aufbau eines sicheren "Tunnel" zwischen dem VPN-Client und dem VPN-Server.
4. Hierzu muss sich der VPN-Client gegenüber dem VPN-Server authentisieren.
5. Erst nach erfolgreicher Authentifizierung wird der verschlüsselte IPsec-Tunnel[44] aufgebaut, über den dann ein abhörsicherer Datenverkehr ins Campusnetz hinein (bzw. von Standort zu Standort) erfolgen kann.

Nach dem Aufbau des Tunnels besitzt der VPN-Client in der Regel keine direkte Verbindung mehr zum Internet (Split-Tunnel sollten aus Sicherheitsgründen unterbunden werden[45]). Der Zugang zum Internet erfolgt nur noch über das Campusnetz. Gleichzeitig bekommt der Client eine IP-Adresse aus dem Hochschulnetz (Intranet) zugewiesen.

---

42 [Schwoch] S. 257
43 [Reichw] S. 73f
44 [Lipp] S. 176
45 [Kappes] S. 213f

Durch den Einsatz eines VPNs könnte ein Computer außerhalb des Campus, so betrieben werden, als ob er sich im Campus befindet, und müsste auch alle Einstellungen, welche im Campus gelten, einhalten. Dieser Computer wäre durch die VPN-Verbindung Teil des Campusnetzes und hätte damit die gleichen Rechte wie alle Hochschulrechner. Beim Aufbau dieser Verbindung erfolgt eine Authentifizierung, so dass nur berechtigte Nutzer über das VPN Zugriff erhalten.

Wie in Kapitel 5 zu sehen ist, nutzen viele Hochschulen diese technische Möglichkeit, um Hochschulangehörigen den Zugang von außen zu gewähren.

Nachteil:

- Lösung für Hochschulbibliothek allein zu komplex
- Endnutzer muss über technisches Prinzip genau unterrichtet werden
- zusätzlich Hemmschwellen durch Installation von weiterer Software und zusätzlichem Konfigurationsaufwand[46]
- diese Anforderungen an Technik und Nutzer schränken die Akzeptanz ein

Derzeit ist ein VPN an der Hochschule Lausitz nur für Administratoren zugelassen. Auch für diese werden nur eingeschränkt Dienste angeboten.

[46] [BuB0210]

6.5 Schlussfolgerung

Es wurden alle Bereiche der Anforderungen analysiert und mögliche Lösungsansätze aufgezeigt. Dabei gibt es sicher noch viele weitere Möglichkeiten die gestellten Teilaufgaben zu lösen. Um die Anforderungen durch eine zeitnahe Lösung zu bedienen, musste teilweise ein pragmatischer Kompromiss geschlossen werden.

6.5.1 Aktualität von Nutzerdaten

Betrachtet man die Referenzen

- TU München[47]
- Uni Heidelberg[48]
- ThULB Jena[49]
- an niedersächsischen Hochschulen[50]

stellt man schnell fest, das diese Projekte hochschul- wenn nicht sogar landesweit mit erheblichen zeitlichen, personellen und finanziellen Kontingenten realisiert wurden. Dabei war die Aktualität der Nutzerdaten nur ein Teilbereich. Trotzdem kann und muss man von diesen Umsetzungen lernen und evtl. gewisse Voraussetzungen schaffen, um die nächsten Schritte anzugehen.

Der IDM-Connector von OCLC, von der Hochschulbibliothek im Rahmen der Systemmigration mit erworben, stellt für zwei der vorhandenen Anforderungen eine optimale Lösung dar. Er wird in immer mehr wissenschaftlichen Einrichtungen als Manager von Nutzerdaten zwischen den verschiedensten Verzeichnisdiensten verwendet. Es könnte also auf einen großen Erfahrungsschatz zurückgegriffen werden.

Die zentralen LDAP-Verzeichnisse der Hochschule Lausitz werden durch die zentrale Nutzerdatenbank aber nur mit Authentifizierungsdaten (Loginname und Passwort) gefüllt. Durch die fehlenden Adressdaten sind die benötigten Voraussetzungen für den Einsatz des IDM-Connectors nicht gegeben. So sollte auf das im Kapitel 6.1.1 beschriebene Skripting zurückgegriffen werden. Da ein bidirektionaler Datenabgleich vom Hochschulrechenzentrum derzeit nicht gewünscht wird und technisch mit der bestehenden Struktur auch nur sehr schwer umsetzbar wäre, sollte vorerst nur die

47 [IM HS]
48 [Lange]
49 Internet: http://www.uni-jena.de/Verzeichnisdienste.html [18.11.2010]
50 [SOI]

vom LBS angebotene Importfunktion automatisiert werden. Somit erhielte man täglich die aktuellen im Studentensekretariat gemeldeten Nutzerdaten und man würde die Bereitstellung im Fremddatenpool erreichen. Ziel sollte es jedoch sein, ein hochschulweites Identitätsmanagement aufzubauen, das einen bidirektionalen Datenaustausch realisiert.

Der Datenimport in das LBS stellt eine einfache und schnell realisierbare Lösung dar. Trotzdem sollte der IDM-Connector von OCLC genauer analysiert und erste Teststellungen eingerichtet werden.

6.5.2 Verzeichnisdienst

Als wichtigstes Ergebnis dieser Betrachtung ist die Notwendigkeit des Aufbaus eines bibliothekseigenen Verzeichnisdienstes anzusehen. Dieser ist mit allen berechtigten Bibliotheksnutzern (internen wie externen) und allen berechtigten Hochschulangehörigen zu füllen. Über diesen Verzeichnisdienst können die Anforderung der Autorisierung beim Zugang zum Internet und Zugriff von außerhalb der Hochschule auf elektronischen Ressourcen behandelt werden.

Im Hochschulrechenzentrum wurde bereits eine Active Directory Struktur aufgebaut. Sie wird aber leider derzeitig als Stand-Alone Domain betrieben und es werden keine Vertrauensstellungen mit dieser gewünscht. Dieses Konzept sollte jedoch beibehalten werden, um eine evtl. spätere hochschulweite Domain-Struktur auf Basis des Active Dirctory Service ohne Systemwechsel einrichten zu können. Der hochschulbibliotheksweite Einsatz von Microsoft Windows XP und die vielseitigen hochschulweiten Erfahrungen unterstützen dieses System. Der Datenimport sollte mit dem SQL2AD-Tool von Seifert erfolgen, da dieses Werkzeug bereits für das Auslesen der zentralen Nutzerdatenbank der Hochschule Lausitz konzipiert wurde. Es müssen jedoch Anpassungen für das Auslesen der LBS-Daten aus einer Sybase-Datenbank getätigt werden.

Durch dieses Verzeichnis wäre es auch möglich Funktionalität und Umsetzbarkeit des IDM-Connenctor zu testen. Um so erste Erfahrungen für den Aufbau eines zentralen Identitätsmanagement mit bidirektionalen Datenaustausch zu sammeln.

6.5.3 Zugang zum Internet an Arbeitsstationen der Hochschulbibliothek

Auf Grund von Missbrauchsvorfällen und Angriffsversuchen in letzter Zeit auf das interne Hochschulnetz wurde festgelegt, dass es eine direkte Anmeldung an den ca. 50 Arbeitsstationen der Hochschulbibliothek geben sollte. Wie eingangs beschrieben,

darf jedoch keine Protokollierung von Logindaten durchgeführt werden. Das macht den Nachweis von eventuellen Missbräuchen und der daraus resultierenden Sperrung für solche Nutzer unmöglich . Sollte es trotz der mentalen Barriere der Anmeldung, zu Missbräuchen kommen, könnten in Abstimmung mit dem Datenschutzbeauftragen der Hochschule Lausitz doch Logindaten kurzzeitig mitprotokolliert werden, um gegenüber dem Rechenzentrum und der Hochschulleitung aussagekräftig zu sein und betreffenden Nutzern den Zugang zu den Arbeitsstationen zu verwehren.

Über einen eventuellen Ausbau dieses Systems durch einen zusätzlichen Bibliotheksproxy mit speziellen Konfigurationen für jede Bibliotheks-Benutzergruppe muss zu einem späteren Zeitpunkt entschieden werden. Dieser sollte nur als Single-Sign-On-Lösung umgesetzt werden, d.h. Anmeldedaten werden auch an den Proxy übertragen.

6.5.4 Zugang zu elektronischen Ressourcen

Shibboleth wird favorisiert wegen der zunehmenden Verbreitung und Akzeptanz, gegebener Single-Sign-On Unterstützung und sichererer Authentifizierung. Hierbei ist dies aber keine schnelle „kleine“ Bibliothekslösung, die von der Hochschulbibliothek allein etabliert werden kann. Nur eine hochschulweite Realisierung ist sinnvoll und sollte zentral im Hochschulrechenzentrum verwaltet werden. Mit der zentralen Nutzerdatenbank und dem angeschlossenen LDAP-Verzeichnis liegt die Grundvoraussetzung vor.

Alternativ sollten die beiden vorgestellten Produkte eines Rewrite-Proxys analysiert werden und damit eine kurzfristige und pragmatische Lösung gefunden werden.

6.5.5 Übersicht

Überträgt man diese Schlussfolgerungen in die Abbildung 18, ergibt sich folgende schematische Aufstellung:

1. Nutzerdaten werden direkt aus der zentralen User-DB in das LBS (Ablösung des manuellen Datenabgleichs) übertragen
2. Aufbau eines Bibliothekseigenen Verzeichnisdienstes als Active Directory, dieses soll zur Authentifizierung an den Arbeitsstationen der Hochschulbibliothek dienen.
3. Automatisches übernehmen von Nutzerdaten aus dem LBS in das Active Directory (2.).
4. Automatisches übernehmen von Nutzerdaten aus der Zentralen User-DB in das Active Directory (2.)
5. Zur Verfügung stellen von elektronische Ressourcen durch einen Rewrite-Proxy, die Authentifizierung erfolgt ebenfalls durch das Active Directory (2.)

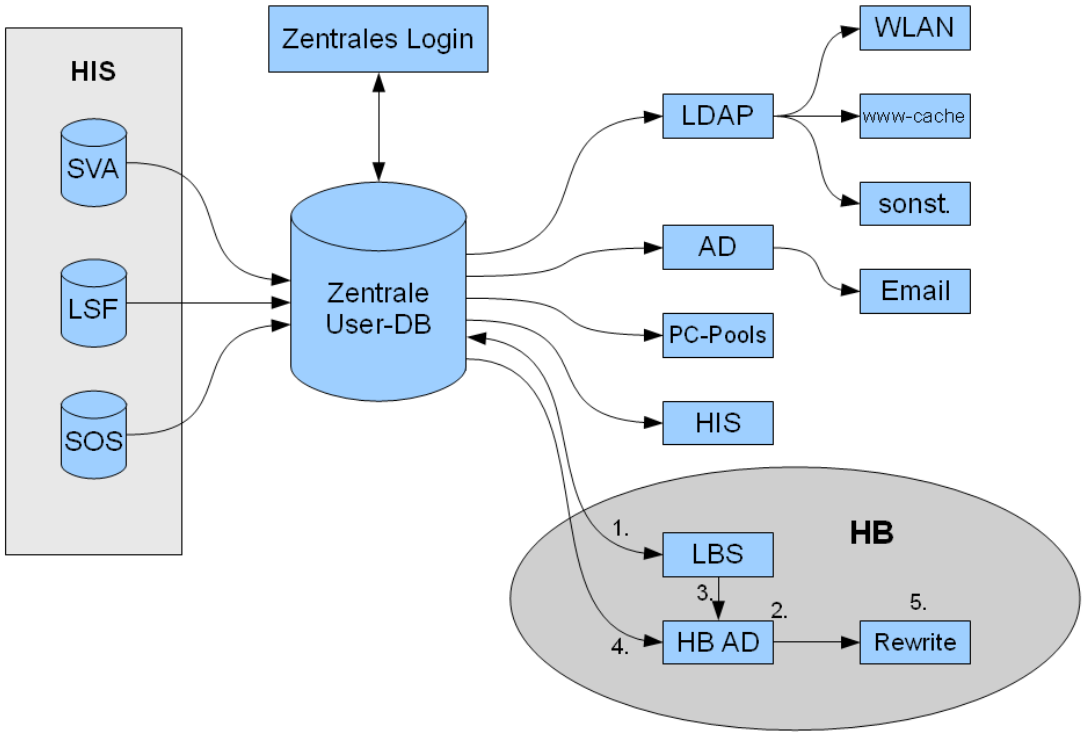

Abb. 18: schematische Übersicht der IuK- Struktur der HL (Ziel)

7 Umsetzung in der Hochschulbibliothek der Hochschule Lausitz (FH)

7.1 Aktualität von Bibliotheksnutzerdaten

7.1.1 Beschreibung des Umfeldes

Die Nutzerdaten werden im lokalen Bibliothekssystem vorgehalten, diese sind auf elf Tabellen verteilt und werden vom Ausleih-Client angesprochen. So steht dem Bibliothekspersonal eine Oberfläche zur Verfügung um evtl. Änderungen dieser Daten durchzuführen, oder die Angaben zu kontrollieren. Aus diesen Tabellen werden auch Mahnbriefe und E-Mails erzeugt.

Für den Datenimport ist die Tabelle d21fremd vom Bibliothekssystem bereits vorgesehen. Der Ausleih-Client ist so konfiguriert, dass bei Eingabe der Matrikelnummer in dieser Tabelle nachgesehen wird, ob dort Nutzerdaten hinterlegt sind.

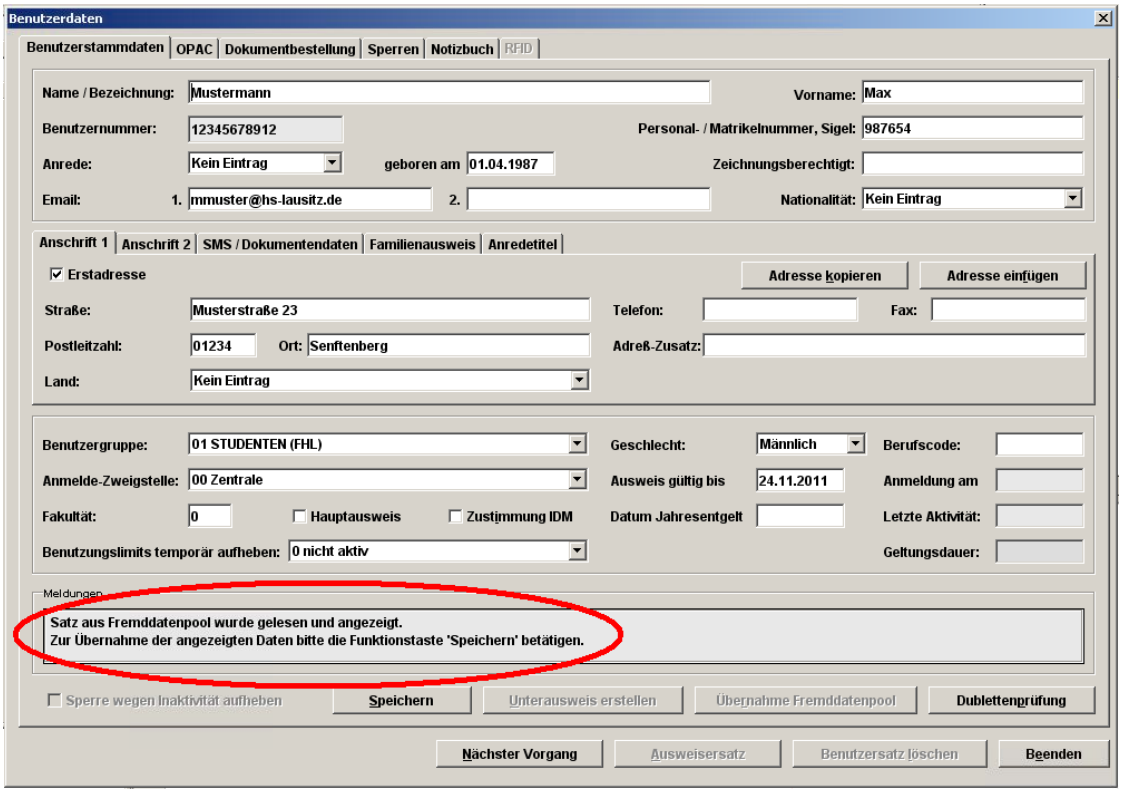

Abb. 19: Ausleih-Client

Wie in Kapitel 3 beschrieben, werden Nutzerdaten der Studenten im Studierendenmanagement HIS-SOS aktuell gehalten. Diese Daten sollten laut Anforderungen der Hochschulbibliothek (Kapitel 4) möglichst tagesaktuell in der Hochschulbibliothek zur Verfügung stehen. Der manuelle Datenabgleich soll durch einen autonomen Datenabgleich ersetzt werden.

Bei diesen Manipulationen ist eine genaue Analyse in Bezug auf das Verhalten der vom Bibliothekssystem bereitgestellten Client-Software (hier vor allem der Ausleih-Client) zu betrachten, und es war eine Rückfrage beim Hersteller zwingend erforderlich gewesen. Zum einen soll der Datentransfer nur in die dafür vorgesehene Tabelle d21fremd stattfinden, aber zum anderen auch in das Notizbuch, welches in der Tabelle d30notiz hinterlegt ist. Der Hersteller OCLC weist ausdrücklich darauf hin, dass eine Massenänderung von Nutzerdaten per SQL nicht empfohlen wird. Aber einem Datenimport in die dafür vorgesehene Tabelle d21fremd steht nichts entgegen. So wurde auf Anraten von OCLC in der ersten Realisierung nur der Fremddatenpool gefüllt.

Für den Datenaustausch wurde ein Format vereinbart – dieses Format spiegelt sich in einer neuen Tabelle d00tmp wieder:

```
create table d00tmp(
 d00bnr varchar (16) NULL ,      /* Benutzernummer          */
 d00vname char (40) NULL ,       /* Vorname                 */
 d00name char (60) NULL ,        /* Nachname                */
 d00o1 char (40) NULL ,          /* Ort                     */
 d00s1 char (40) NULL ,          /* Strase                  */
 d00p1 char (12) NULL ,          /* Postleitzahl            */
 d00anschr varchar (101) NULL ,  /* Anschriftenzusatz       */
 d00tel char (20) NULL ,         /* Telefonnummer           */
 d00anrede smallint  NULL ,      /* Anredeschluessel        */
 d00gedatum datetime  NULL ,     /* Geburtsdatum            */
 d00sp1 smallint  NULL ,         /* Sperre 1                */
 d00sp2 smallint  NULL ,         /* Sperre 2                */
 d00sperre1 datetime  NULL ,     /* Sperrdatum 1            */
 d00sperre2 datetime  NULL ,     /* Sperrdatum 2            */
 d00aufart smallint  NULL ,      /* Aufnahmeart             */
 d00fremd_nr char (11) NULL ,    /* Personal Matrikel Siegelnummer*/
 d00datauf datetime  NULL ,      /* Aufnahmedatum           */
 d00zweig smallint  NULL ,       /* Zweigstelle             */
 d00bg smallint  NULL ,          /* Benutzergruppe          */
 d00sex char (1) NULL ,          /* Geschlecht              */
 d00nation char (3) NULL ,       /* Nation                  */
 d00fakul smallint  NULL ,       /* Fakultaet               */
 d00z_str char (40) NULL ,       /* Zweit-Strasse           */
 d00z_plz char (12) NULL ,       /* Zweit-Plz               */
 d00z_ort char (40) NULL ,       /* Zweit-Ort               */
 d00z_anschr varchar (101) NULL, /* Zweit-Anschriftenzus.   */
 d00z_tel char (20) NULL ,       /* Zweit-Telefonnummer     */
 d00email1 varchar (255) NULL    /* email 1                 */
 )
with identity_gap = 1000
```

Die Datentypen dieser neuen Tabelle sind identisch mit den ersten 28 Spalten der Tabelle d21fremd, welche über weitere 15 Spalten verfügt. Diese Werte können aber durch das HRZ nicht zur Verfügung gestellt werden, bzw. werden in der Hochschulbibliothek nicht ausgewertet.

7.1.2 Zielbeschreibung

Es werden im HRZ Daten bereitgestellt, welche der beschriebenen Tabelle d00tmp entsprechen. Diese Daten sollen in regelmäßigen Abständen in der Hochschulbibliothek eingespielt und in der dafür vorgesehenen Tabelle d21fremd aktualisiert werden.

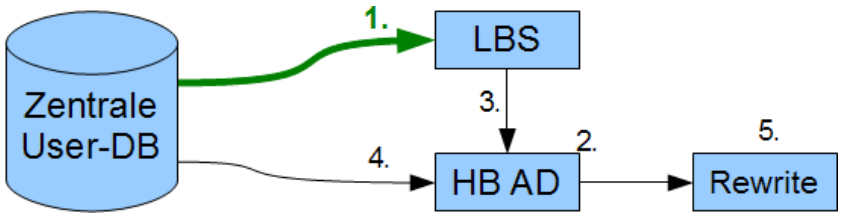

Abb. 20: Schematische Übersicht der IuK- Struktur der HL – Punkt 1

7.1.3 Realisierung

Für den Datentransfer zwischen zwei SQL-Datenbanken wäre ein Programm SQL2SQL vorteilhaft, um Daten ähnlich dem Tool SQL2AD direkt aus verschiedenen Datenbanken in eine andere Datenbank zu übertragen. Aus zeitlichen Gründen wird im Anhang nur eine Spezifikation dieser Software erstellt.

Für diese Arbeit wird eine in der Hochschule langjährig eingesetzte Lösungsvariante angepasst. Hierzu wird mindestens 1x am Tag ein aktueller Datenbankexport der zentralen Nutzerdatenbank im HRZ mit allen relevanten Nutzerdaten erstellt. Diese Datei wird verschlüsselt von HRZ-Server zum HB-Server übertragen. Der anschließende Import erfolgt mittels dem von OCLC im Bibliothekssystem bereitgestellten Datenbanktool dbtool[51], welches die Daten in die oben beschriebene temporäre Tabelle überträgt. So werden die Daten für eine weitere SQL-Verarbeitung in der Tabelle d00tmp bereitgestellt. Mit dieser Tabelle kann nun der Fremddatenpool und somit die d21fremd gefüllt werden.

[51] Internet: http://mikiwiki.org/wiki/Sybase#dbtool [27.11.2010]

7.1.4 Ergebnisse und Aussicht

Der ursprüngliche Wunsch, die Adressdaten zu übernehmen, wurde aus drei Gründen verworfen:

1. Es kann vom HRZ nur noch die Hauptadresse geliefert werden, da die Zweitadresse nicht in der zentralen Nutzerdatenbank gespeichert wird. Diese ist nur im Studierendenmanagement HIS-SOS vorhanden, wird nicht abgeglichen und steht somit der Hochschulbibliothek nicht zur Verfügung.
2. Eindringliche Warnung von OCLC, keine Massenänderung von SQL-Daten durchzuführen.
3. Das Ausleihpersonal hat die Möglichkeit, die zentral gemeldete Hauptadresse jederzeit einzusehen und so einen manuellen Adressvergleich durchzuführen.

7.2 Zugang zu den Arbeitsstationen

7.2.1 ADS & SQL2ADSeifert

Als Verzeichnisdienst wurde ein Windows 2008 Server als virtuelle Maschine auf einem Linux-xen-System mit zugewiesenen 512MB RAM, 1x 2,4GHz Prozessor und 30 GB Festplattenspeicher aufgesetzt.

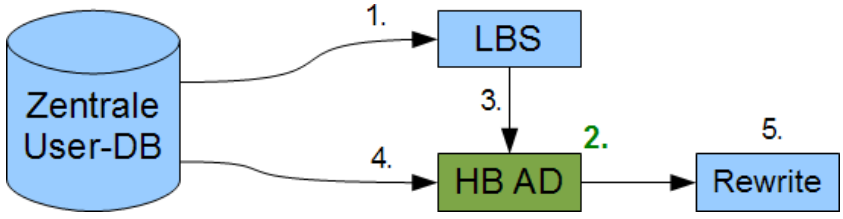

Abb. 21: Schematische Übersicht der IuK- Struktur der HL – Punkt 2

Auf diesen ADS Server wurde das SQL2AD-Tool laut Handbuch installiert. Um die Anforderungen „Aufbau eines bibliothekseigenen Verzeichnisdienstes mit Zugangsdaten aus dem LBS und der zentralen Nutzerdatenbank“ zu realisieren, mussten Daten aus zwei verschiedenen Quellen ausgelesen werden.

7.2.2 Zugriff auf Bibliotheksnutzerkonten des LBS

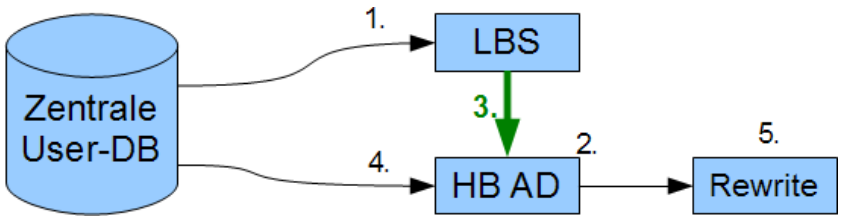

Abb. 22: Schematische Übersicht der IuK- Struktur der HL – Punkt 3.

Zur einfacheren Bereitstellung der Nutzerdaten und der Verzeichnisstruktur wurden die benötigten Daten in zwei neu erstellten Views in der Sybase-Datenbank bereit gestellt.

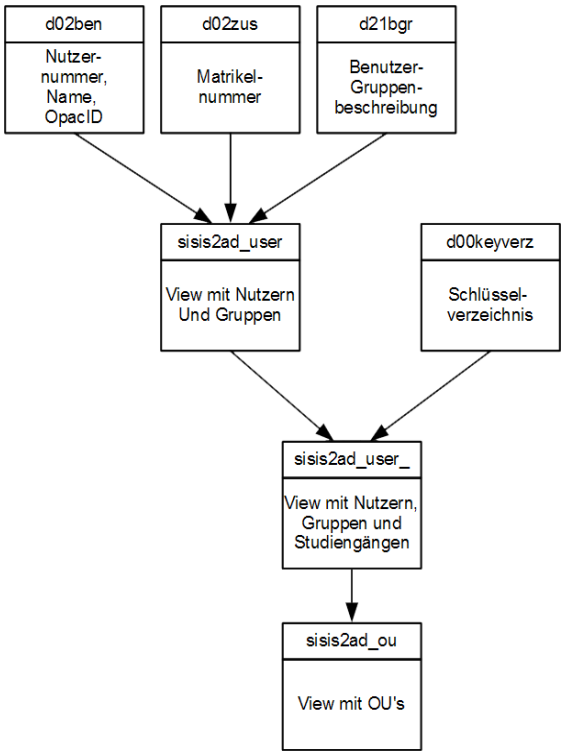

Abb. 23: Viewsübersicht für SQL2AD

Wie in Abbildung 23 zu sehen ist, wird der View sisis2ad_user aus den Standardtabellen d02ben, d02zus und d21bgr des LBS erstellt. Dieser beinhaltet damit nur die notwendigen Informationen für eine Weiterverarbeitung mit dem Programm SQL2AD. Diese sind: ou (Studiengang), superou (Benutzergruppe), Benutzernummer, Name, Vorname, Opac-ID (bibliotheksinternes Passwort).

```
create view sisis2ad_user as
      select       d02zus.d02beruf as ou,
             d21bgr.d21gruppe as superou,
             d02ben.d02name+', '+d02ben.d02vname as printablename,
             d02ben.d02bnr as loginid,
             d02ben.d02vname as vorname,
             d02ben.d02name as name,
             d02ben.d02opacpin as opacid,

             from d21bgr, d02ben

             where  d02ben.d02bg=d21bgr.d21bgr and
                    d02ben.d02opacpin <> '' and      -- nur mit opacid
                    d02ben.d02awdatum >=CURRENT_DATE() and
                                       -- mit noch gueltigen Nutzerausweis
                    d02ben.d02internet <>'N' and
                                       -- welche Zugangsberechtigt sind
                    (d02ben.d02bg <6 or -- aus den Benutzergruppen 1-5
                    d02ben.d02bg >9)    -- und 10-12
```

Es werden in dem Datenbank-View nur Nutzer angezeigt, welche:

- angemeldete Bibliotheksnutzer sind
- eine vergebene OpacID besitzen
- einen gültigen Nutzerausweis haben
- und die Berechtigung für den Internetzugang besitzen.

Alle vier Ereignisse können durch die BibliotheksmitarbeiterInnen mit dem Ausleih-Client von OCLC-SunRise behandelt werden.

Da in den Standardtabellen der verwendete Berufscode (in welchen die Schlüsselverzeichnisnummer des Studienganges eingetragen wird) in nummerischer Form hinterlegt ist und sich diese nummerische Darstellung im AD als unübersichtlich erwies, wurde eine weitere Tabelle erzeugt und herangezogen, in der eine alphanumerische Ersetzung eingepflegt wurde.

```
-- d00keyver neue Tabelle mit Schlüsselverzeichnis => Studiengangsübersicht
create table d00keyver (d00key char(4), d00stg char(40))
```

Mit diesen Daten (siehe Anhang) war es nun möglich, einen komplett alphanumerischen View in der Datenbank zu erzeugen, in welchem der Fachbereich klar erkennbar ist.

```
-- sisis2ad_user_  View mit Beschreibung der Fachbereiche
create view sisis2ad_user_ as
      select d00stg as ou, superou, printablename, loginid, vorname, name,
              opacid from sisis2ad_user, d00keyver where d00key=ou
             union
      select * from sisis2ad_user
             where ou not in (select d00key from d00keyver)
```

Diese Tabelle bildet die Grundlage für den View sisis2ad_ou, welcher aus den bereitgestellten Nutzerdaten die Baumstruktur der Nutzergruppen und Fachbereiche erstellt.

Mit Hilfe der SQL2AD-Gui wurden zwei XML Steuerdateien erzeugt:

1. view_ouSisisToADS.xml erstellt und aktualisiert die Baumstruktur im ADS
2. view_userWithOuSisisToADS.xml trägt die berechtigten Nutzer in jeweilige Gruppen des ADS ein und löscht diese ggf.

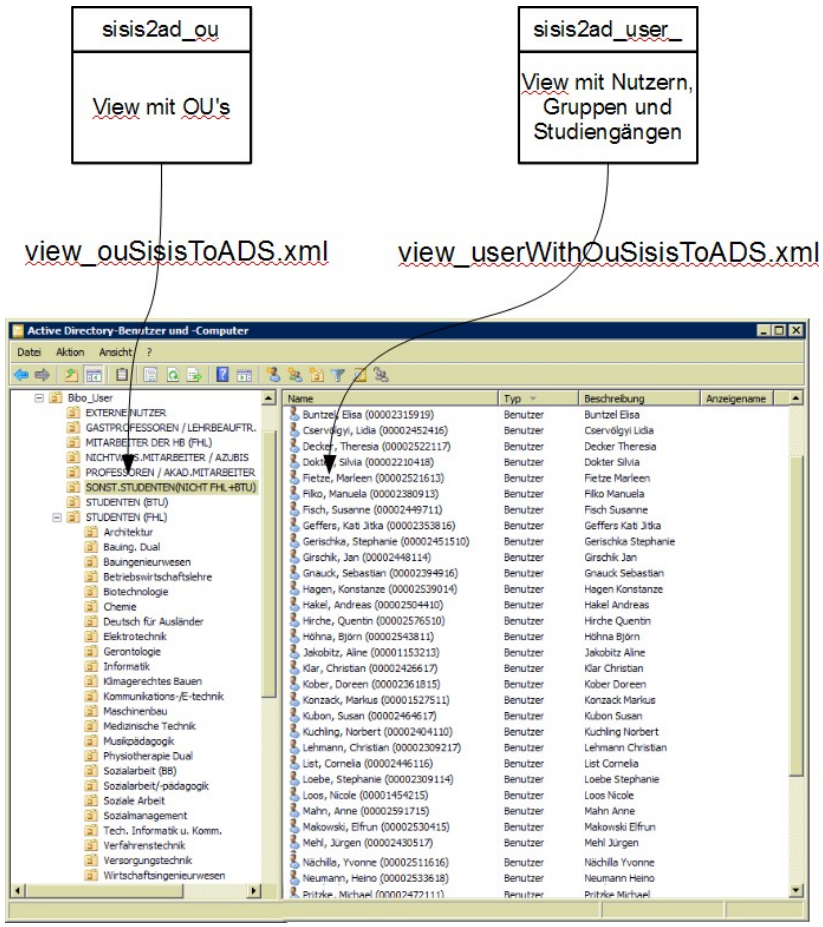

Abb. 24: Funktionsübersicht für SQL2AD-Bibliotheksnutzer

Beide Steuerdateien müssen nacheinander ausgeführt werden, erst nach erfolgreicher Überarbeitung der Baumstruktur, können die berechtigten Nutzer in diese eingetragen werden. Der Aufruf dieser beiden SQL2AD–XML-Steuerdateien wurde so eingestellt, dass während der Öffnungszeiten der Hochschulbibliothek ein Datenabgleich aller 15 Minuten stattfindet. Somit ist die gewünschte zeitnahe Aktualität gegeben. Hierzu wurde ein cron-Dienst für Windows[52] eingerichtet.

[52] nnCron LITE Internet: http://www.nncron.ru/ [27.11.2010]

```
# alle 15 min - von 8-19 Uhr - Mo-Sa Nutzer aus sisis Laden
*/15 8-18 * * 1-6 "c:\!!sisis2AD\start-sisis.bat"
```

mit Inhalt:

```
cd \!!sisis2AD\
java -jar sqlToAd.jar -run view_ouSisisToADS.xml
java -jar sqlToAd.jar -run view_userWithOuSisisToADS.xml
```

Erste Aktualisierungen der Nutzerdatenbank dauerten ca. 5 Minuten. Diese Performance konnte durch das Heraufsetzen der zugewiesenen Hardware – Ressourcen auf 1GB RAM und 2x2,4 Ghz Prozessoren für die virtuelle Maschine auf unter 1 Minute gesteigert werden.

7.2.3 Zugriff auf zentrale Nutzerdatenbank im HRZ

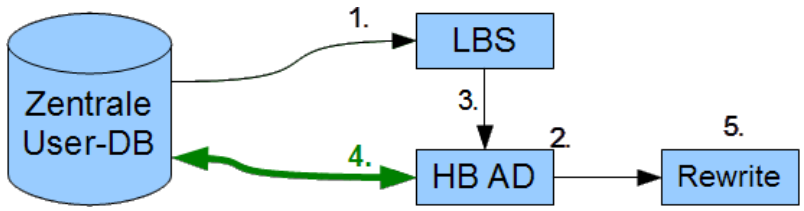

Abb. 25: Schematische Übersicht der IuK- Struktur der HL – Punkt 4

Da nur berechtigte Bibliotheksnutzer Zugang zu den an das Active Directory angeschlossenen Diensten haben sollen, wurde das in der zentralen Nutzerdatenbank vorgesehene Feld „Bibliothekskennung“ benutzt und mit der entsprechenden Bibliotheksnutzernummer gefüllt. Damit wird dem Nutzer in der zentralen Nutzerdatenbank das Merkmal „berechtigter Bibliotheksnutzer“ zugewiesen. So ist es möglich nur Nutzer aus der zentralen Nutzerdatenbank auszulesen, welche auch in der Bibliothek zugangsberechtigt sind.

Es wurde erneut ein Datenbank-View im LBS erstellt. Dieser weist einer Matrikelnummer nur die dazugehörige Bibliotheksnummer zu, wenn folgende Bedingungen erfüllt sind:

- Nutzer mit Matrikelnummer ist in Bibliothek gemeldet
- Berechtigung für das Internet ist gesetzt
- gültiger Nutzerausweis ist vorhanden

```
/*==============================================================*/
/* View: USERANDMATR                    */
/*==============================================================*/
create view USERANDMATR as
select
  d02ben.d02vname,
  d02ben.d02name,
  d02ben.d02gedatum,
  d02ben.d02bnr,
  d02zus.d02fremd_nr
from
  d02ben,
  d02zus
where
  d02ben.d02bnr = d02zus.d02z_bnr
  and d02zus.d02fremd_nr <> ''
  and d02ben.d02bg < 5
  and d02ben.d02awdatum >= CURRENT_DATE()
  and d02ben.d02internet <> 'N'
go
```

Diese Daten werden per dbtool in eine Datei exportiert, per sicherem Datentransfer ins Rechenzentrum übertragen und dort per Script in die zentrale Nutzerdatenbank eingepflegt.

In der derzeitigen Anfangsphase wurden folgende Termine festgelegt:

- 19:30 Uhr Auslesen der berechtigten Nutzer aus dem LBS und Übermittlung in das HRZ
- 22:10 Uhr Einlesen dieser Daten in die zentrale Nutzerdatenbank
- 07:30 Uhr Einlesen der Nutzerdaten aus dem HRZ und Einpflegen in das Bibliotheks–ADS.

Im HRZ werden für diesen Datenimport ebenfalls 2 Datenbank–Views von der zentralen Nutzerdatenbank bereitgestellt und können so über SQL2AD–XML-Konfigurationsdateien abgerufen werden.

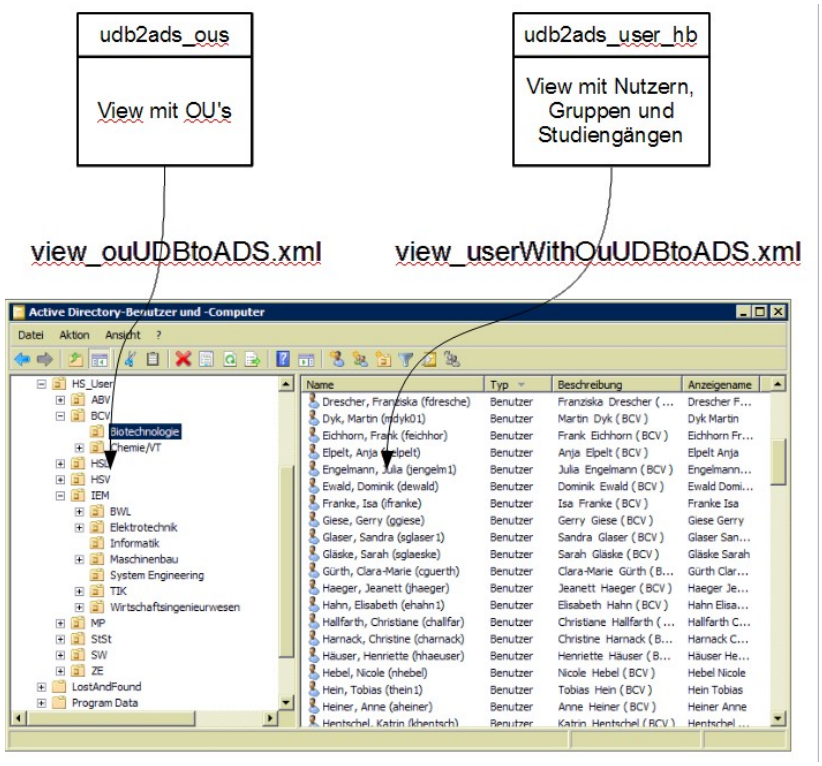

Abb. 26: Funktionsübersicht für SQL2AD-Bibliotheksnutzer

7.2.4 Ergebnisse und Aussicht

Ergebnisse:

- Erste Teststellungen wurden an beiden Standorten eingerichtet.
- Einweisung des Bibliothekspersonals ist erfolgt

Aussicht:

- Einrichten an allen öffentlich zugänglichen Arbeitsstationen (ca. 35) der Hochschulbibliothek ist bis zum Beginn des SS 2011 vorgesehen.
- Abgleich mit zentraler Nutzerdatenbank soll mehrmals täglich durchgeführt werden.
- Je nach Nutzergruppe könnte ein Proxy mit verschiedenen Black/Withe-List zusätzlich aufgebaut werden (z.B. Uni Rostock[53]), um die Zugänge zu elektronischen Ressourcen weiter zu differenzieren.

[53] [Siman] S. 52 - 57

7.3 Authentifizierter Zugang zu elektronischen Ressourcen

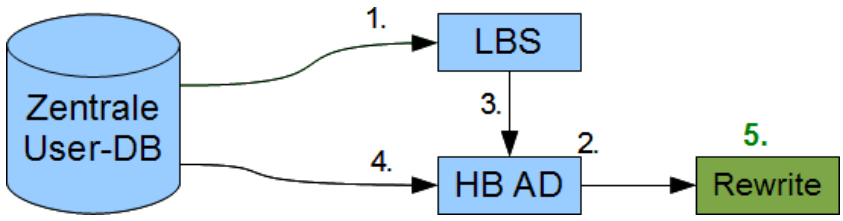

Abb. 27: Schematische Übersicht der IuK- Struktur der HL – Punkt 5

Es wurde eine zweimonatige Testphase mit den vorgeschlagenen Produkten (HAN und EZProxy) gestartet. Dazu wurden von beiden Herstellerfirmen Testsysteme bzw. Testlizenzen zu Verfügung gestellt.

Um beide Produkte vergleichen zu können, wurden folgende Punkte festgelegt:

1. Konfigurieren, an Hochschule anpassen und starten
2. Einbinden des vorhandenen AD-Systems
3. Anpassen der Login-Seite
4. Bereitstellen von mindestens zwei elektronischen Ressourcen
5. Zugriff von einem internen Rechner ohne eigene Proxyeinstellung
6. alternative Authentifizierung (IP-Adresse, LBS oder andere)
7. Lizenzmanagement
8. Auswertung der Statistik / Logfiles
9. Anfrage im HRZ über Freigabe in der Firewall bzw. DNS-Eintrag
10. Testzugriffe von außen

7.3.1 EZ Proxy mit Test - Lizenzschlüssel

Eine Testversion steht für jedermann auf der Internetseite[54] von OCLC zur Verfügung. Unproblematisch lässt sich ein Lizenzschlüssel für eine 30 Tage-Testversion von der Amerikanischen-OCLC-Hotline anfordern und aktivieren. Als Testsystem wurde ein Windows XP Professionell gewählt, welches als xen-virtuelle-Maschine mit bereitgestellten 1GB Ram, 1x 2,4GHz Prozessor und 10GB

[54] Internet: http://www.oclc.org/de/de/support/documentation/ezproxy/evaluation.htm [17.11.2010]

Festplattenspeicher eingerichtet wurde. Mit Hilfe der Anleitung auf der Internetseite des EZ-Proxy sind die benötigten Anpassungen in config- und HTML-Dateien schnell realisiert. Über das Administrationsmenü lassen sich dann folgende Informationen und Einstellungen abrufen:

- derzeitige Aktivität
- Logfiles mit teilweise einfacher statistische Aufbereitung
- ein Restart des EZ-Proxy ist möglich
- SSH Zertifikat Einrichtung und Erstellung
- Test der Nutzerauthentifikation
- Test des Netzwerkzuganges
- Einstellungen für Shibboleth
- Einstellungen für die LDAP-Anbindung

Über den letzten Punkt lässt sich der EZ-Proxy sehr einfach an ein bestehendes LDAP-System anbinden. Durch Eintragen der individuellen Parameter, werden die benötigten Konfigurationszeilen generiert.

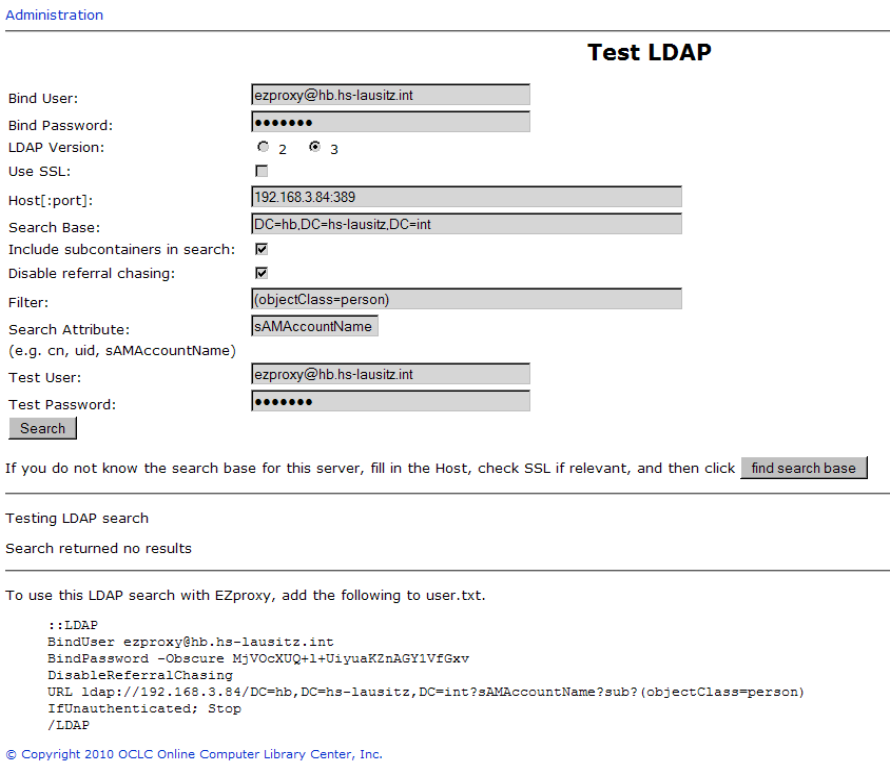

Abb. 28: LDAP Konfiguration des EZ-Proxy

Der EZ-Proxy kann in zwei unterschiedlichen Modi arbeiten. Zum einem „Proxy by Port“ und „Proxy by Hostname“. Diese beiden Modi verlangen eine differenzierte Behandlung in der Firewall.

In „Proxy by Port“ wird die Kommunikation jeder bereitgestellten elektronischen Ressource über einen eigenen zugewiesenen Port abgewickelt. In diesem Fall besteht die Problematik in der Konfiguration der Firewall. Bei jeder neu eingetragenen elektronischen Ressource müssen weitere Ports vom HRZ freigeschaltet werden. Eine direkte EZ-Proxy by Port URL würde so aussehen:

http://ezproxy.domain.de:2050

Im Modus „Proxy by Hostname“ erfolgt die Kommunikation über den Standardport 80 für HTML-Kommunikation. Hierbei sind keine Änderungen in der Firewall notwendig. Es werden dazu nur zwei Einträge im DNS-Server verlangt:

```
ezproxy.domain.de       IN A IP-Adresse
*.ezproxy.domain.de     IN A IP-Adresse
```

Eine direkte EZ-Proxy by Hostname URL würde so aussehen:

http://www.springerlink.de.ezproxy.domain.de

Das Anpassen der Login-HTML-Seiten und das Einbinden der elektronischen Ressourcen geht ähnlich schnell. Für die Ressourcen benötigt man nur die Start-URL und die dazugehörigen Domainnamen, die erlaubt sind. Diese trägt man in der config.txt/ezproxy.cfg ein, z.B.:

```
#Title Name der Ressource fuer Anzeige auf der Internetseite
#U Start-Url
#DJ Domainname

Title google
U http://www.google.de
DJ google.de
DJ test.de
```

Auf allen Seiten der eingetragenen Domain kann über den EZ-Proxy zugegriffen werden. Verlässt man diesen Domainnamen, verlässt man die Umleitung über den EZ-Proxy. In dem oben gezeigten exemplarischen Beispiel könnte man in Google frei suchen und Treffermengen ansehen, wenn sie den Domainnamen test.de beinhalten. Mit einer anderen URL würde man die Kommunikation über den EZ-Proxy verlassen.

Eine echte Authentifizierung über IP-Adresse wird vom EZ-Proxy nicht unterstützt, aber es können IP(-Bereiche) festgelegt werden, welche den EZ-Proxy nicht zu nutzen brauchen. So kann mit der direkten EZ-Proxy-URL von solch einer IP auch ohne eine Authentifizierung auf die Ressource zugegriffen werden.

Andere in der Hochschule verfügbaren Dienste, z.B. FTP und POP konnten ebenfalls erfolgreich abgefragt werden. Hierzu ist teilweise nur eine zusätzliche Zeile in der Konfiguration notwendig.

Eintrag in der Datei user.txt/ezproxy.usr für Authentifizierung gegen FTP Dienst:

```
::ftp=leo.fh-lausitz.de
```

Lizenzmanagement (s. Punkt 7) ist mit EZ-Proxy nicht realisierbar, hier überlässt OCLC dem Datenbankanbieter die Kontrolle.

Für die Auswertung (s. Punkt 8) bietet der EZ-Proxy im Administrationsmenü kaum Möglichkeiten an, nur der aktuelle Serverstatus und die Einsicht in die Logfiles sind möglich.

Für die Zeit der Testphase war es dem HRZ jedoch nicht möglich, die benötigten Freischaltungen von Ports in der Firewall oder die DNS-Eintragungen durchzuführen. Dadurch konnten keine Zugriffe von außerhalb durchgeführt und getestet werden.

Vorteile:

- sehr geringe Hardwareanforderung (min. Pentium II 400MHz)
- sehr geringe Speicherplatzanforderung <7 MB
- Software verfügbar für Windows ab 2000, Linux und Sun Solaris ab Version 8
- einfache Konfiguration
- Anbindung an unterschiedlichste Authentifizierungsdienste (z.B.: LDAP, POP, IMAP, FTP, Shibboleth, RADIUS uvm.)
- Gruppenbildung möglich (nur bestimmten Nutzergruppen besitzen die Berechtigungen für den Zugriff auf einzelne elektronische Ressourcen)
- Basiseinstellung umfasst 500 parallele Zugriffe
- geringe jährliche Kosten

Nachteile:

- kein Lizenzmanagement
- keine Nutzungsstatistik

7.3.2 HAN Demo als VMWare-Image-Player

Von H+H wurde ein Testsystem als VMWare Image mit einem Windows 2008 R2 x64 System und HAN 2.31 mit 5 concurrent Lizenzen bereitgestellt. Es wurde auf einem leistungsstarken modernen Rechner mit Intel i7 Quadcore 2,7GHz Prozessor, 12GB Ram, 1TB Fesplatte und Windows7 64-Bit gestartet. Diese Hardware wurde von Fachbereich Informatik, allerdings nur außerhalb der Vorlesungszeiten zur Verfügung gestellt. Der Testzeitraum beträgt 90 Tage.

In diesem Falle beinhaltet das Anpassen an das lokale Umfeld nur das Eintragen der Proxy-Daten. Alle anderen Einstellungen wurden bereits mit dem Testsystem geliefert.

HAN arbeitet als Proxy by URL, was den Vorteil von keinen bzw. minimalen Einstellungen in Firewall beinhaltet. Hierbei stellt:

`http://han.domain.de/www.springerlink.de`

eine direkte URL auf die durch HAN bereitgestellte elektronische Ressource von Springerlink dar.

Die Einstellungen für die Authentifizierung gegen den vorhandenen Bibliotheks-AD sind über: *HAN Einstellungen-Authentifizierung-Authentifizierungsdienst* schnell und unkompliziert realisierbar.

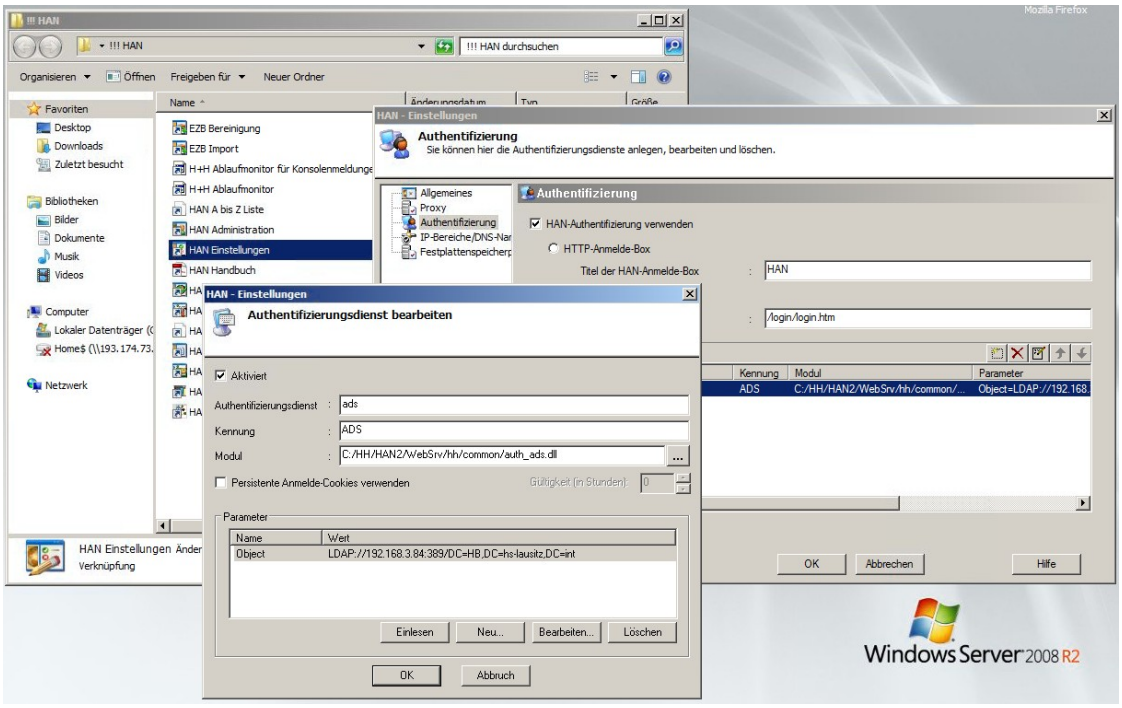

Abb. 29: ADS- Konfiguration von HAN

Über einen zuvor in den HAN-Einstellungen definierten IP Bereich lässt sich eine IP-Authentifizierung durchführen. Die Authentifizierungskriterien werden der eingestellten Reihe nach abgearbeitet. Für jede eingebundene Ressource lassen sich in der HAN-Administration viele weitere Einstellungen tätigen (ua. Lizenzmanagement, Subskriptionsmanagement, EZB-Kommunikation usw.).

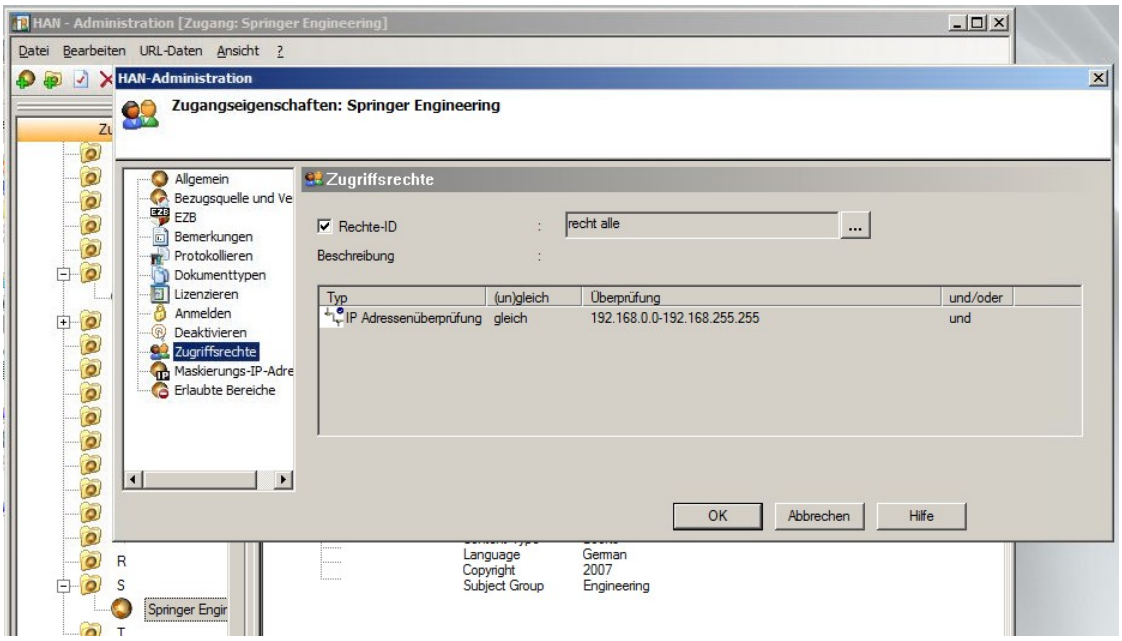

Abb. 30: Ressourcen-Administration in HAN

Durch die eingeschränkte Benutzungszeit konnte keine Freischaltung in der Firewall im HRZ beantragt werden. Ein Zugriff von außen wurde somit auch nicht getestet.

Vorteil:

- Vielzahl von Authentifizierungsmöglichkeiten (IP, LDAP, ADS, NT, ODBC, SISIS, Pica)
- Lizenzmanagement
- Zugriffsrechtemanagement/Nutzerdifferenzierung
- Passwortmanagement für elektronische Ressourcen
- EZB Anbindung
- umfangreiche Nutzungsstatistiken
- Subskriptionsmanagement (Befristungen von Zugängen)

Nachteil:

- begrenzte Anzahl von gleichzeitigen Zugriffen
- hohe einmalige Kosten (Hardware, Betriebssystem, HAN und Zugriffslizenzen)
- hohe Systemanforderungen (z.B. Intel Xeon QC mit 4GB Ram und Win2003 oder Win2008 Serverlizenz)

7.3.3 Ergebnisse und Vergleich

Beide Systeme waren schnell für die Belange der Bibliothek angepasst und konnten umgehend ersten Tests unterzogen werden. Die Vor- und Nachteile beider Produkte sind eindeutig zu erkennen.

Mit HAN erwirbt man ein durchdachtes und vielseitiges Produkt, welches alle Zugriffsarten von elektronischen Ressourcen, eine Vielzahl von unterschiedlichen Nutzerauthentifizierung beherrscht und das Nutzerverhalten sehr komfortabel auswerten lässt. Gegen HAN als Übergangslösung sprechen der einmalige recht hohe Anschaffungspreis und die benötigten Hardwarevoraussetzungen.

EZ-Proxy überzeugt durch dessen Produktschlankheit und kleinen Preis. Er könnte als Übergangslösung, aber auch Dauerbetrieb (durch Jahreslizenzierung und Produktupdates) Einsatz finden. Den größten Nachteil stellt die mangelhafte Statistik dar. Mit dieser sind keine Aussagen über das Nutzerverhalten zu treffen. Da aber derzeit alle Zugriffe auf Datenbanken über das Datenbank-Infosystem[55] (DBIS) der Universität Regensburg laufen und über dieses Zugriffsstatistiken erstellt werden, wird dieser Nachteil abgeschwächt.

Das Aussehen lässt sich für den Endanwender für beide Produkte identisch über HTML-Dateien steuern, so dass ein Wechsel zwischen beiden Produkten für den Endnutzer kaum erkennbar wäre. Die Grundfunktionalität und somit die Anforderungen der Hochschulbibliothek werden durch beide Lösungen erfüllt.

Der Aufbau von Shibboleth sollte jedoch forciert werden. Die Notwendigkeit von dieser Realisierung wird durch den Einsatz des EZ-Proxy bzw. HAN nicht aufgehoben.

[55] Internet: www.bibliothek.uni-regensburg.de/dbinfo/ [03.12.2010]

8 Fazit / Ausblick

Alle drei Anforderungsbereiche

- Sicherung der Aktualität von Bibliotheksnutzerdaten
- Kontrollierter Zugang zu den Arbeitsstationen
- Authentifizierter Zugang zu elektronischen Ressourcen

wurden analysiert und mögliche Lösungen aufgezeigt. Hierbei wurde vor allem auf eine pragmatische, schnelle und gesamtheitliche Lösung für die Hochschulbibliothek Wert gelegt:

- Es sollte das Mehrfacherfassen von Studentendaten unterbunden werden.
  Vom ursprünglichen Ansatz, die Studentendaten direkt aus der zentralen Nutzerdatenbank der Hochschule in das Bibliothekssystem zu übertragen, wurde Abstand genommen, weil damit nur der Hauptwohnsitz des Studenten transferiert werden kann und weil der Entwickler (OCLC) des Bibliothekssystems vom direkten SQL-Datenimport ohne Einsatz des IDM-Connectors (s. Kapitel 6.2.2) abgeraten hat.
  Deshalb erfolgt die indirekte Übernahme ausgewählter, für die Hochschulbibliothek relevanter Studentendaten aus der zentralen Nutzerdatenbank der Hochschule in das Bibliothekssystem. Dazu wird ein Fremddatenpool im Bibliothekssystem genutzt.
  Das Procedere wurde getestet und wird seit Dezember 2010 praktisch angewendet.

- Es sollte ein möglichst unkomplizierter, kontrollierter Internet-Zugang an den öffentlichen Arbeitstationen der Hochschulbibliothek eingerichtet werden.
  In dem Zusammenhang mussten die Anforderungen an die Benutzungsberechtigung und Möglichkeiten der Authentifizierung festgelegt werden.
  Dazu wurde auf einem bibliothekseigenen Server ein Verzeichnisdienst mit Authentifizierungsdaten aus der zentralen Nutzerdatenbank und dem lokalen Bibliothekssystem eingerichtet.
  Im Dezember 2010 sind in der Hochschulbibliothek Testarbeitsplätze eingerichtet worden, und es ist vorgesehen, mit Beginn des SS 2011 diesen kontrollierten Zugang an allen vorhandenen Internetarbeitsstationen zu realisieren.

- Es sollte ein Lösungsansatz für den externen Zugang zu den von der Hochschulbibliothek erworbenen elektronischen Ressourcen gefunden werden.
  Dazu wurden die beiden im Bibliothekswesen verbreiteten Softwareprodukte EZ-Proxy und HAN in Teststellungen miteinander verglichen. Beide sind sowohl technisch-organisatorisch als auch haushaltstechnisch im Jahr 2011 realisierbar.

Um die Arbeit in der Hochschulbibliothek wirksam zu unterstützen und um weitere Erfahrungen sammeln zu können, müssen diese Lösungen tatsächlich im vorgeschlagenen Zeitraum umgesetzt werden.

Natürlich bilden diese Lösungen und Teststellungen nur eine Grundlage für die weitere Entwicklung der IuK-Struktur an der Hochschule Lausitz.

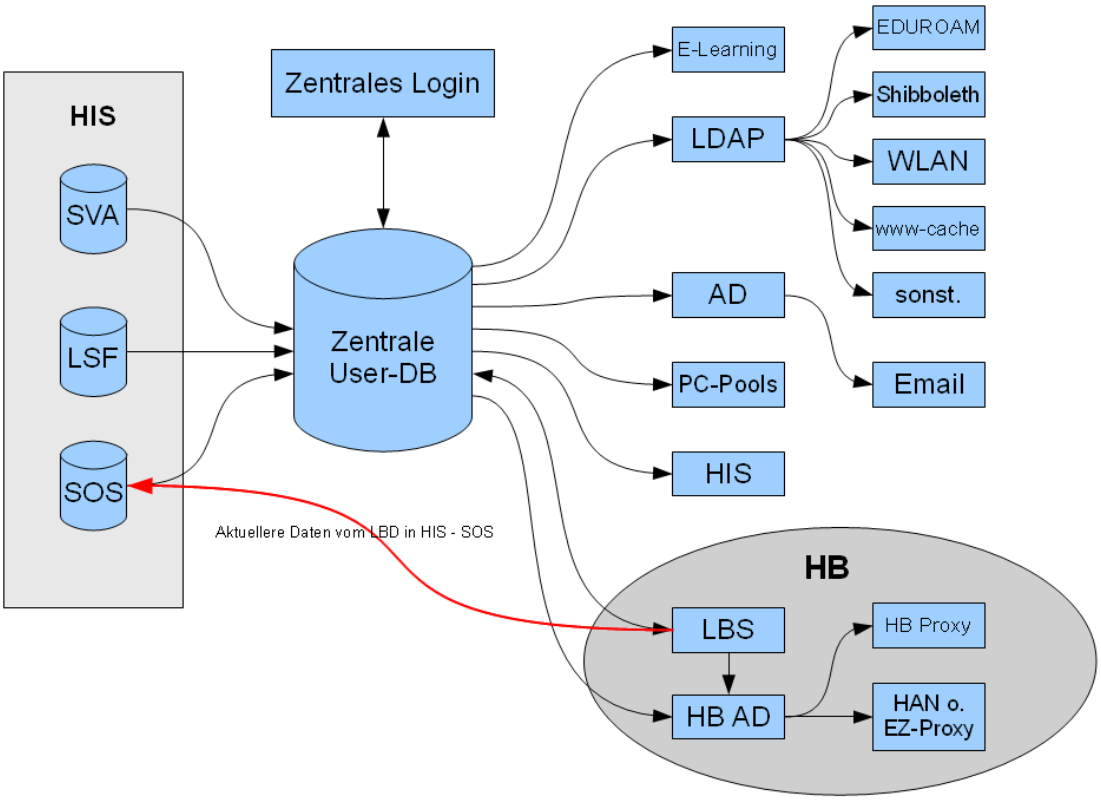

Abb. 31: Vorschlag einer zukünftigen Ausbaustufe der IuK-Technik der HL

Durch die aufgezeigte mögliche gesamtheitliche IuK-Struktur der Hochschule und der darin eingebundenen Hochschulbibliothek – wie in dieser Arbeit gefordert - lassen sich weitere Entwicklungen und Dienste in Angriff nehmen. Bezogen auf die Hochschulbibliothek muss es in allen drei untersuchten Bereichen auch eine Weiterentwicklung geben.

Hierzu zählt:

- Analyse und Aufbau eines bidirektionalen Nutzerdatenaustauschs zwischen den Bereichen: Studentensekretariat, Personalabteilung, Rechenzentrum und Hochschulbibliothek. Ein erster Lösungschritt könnte ein Datentransfer vom LBS in die Studentenverwaltung sein.
- Aufsetzen eines bibliothekseigenen Proxys, um Zugänge zum Internet für die verschiedensten Nutzergruppen weiter zu differenzieren.
- Zentraler Aufbau von Shibboleth und EDUROAM[56] im HRZ, um einen weltweiten Zugriff auf die von der Hochschulbibliothek der Hochschule Lausitz lizenzierten und zur Verfügung gestellten elektronischen Ressourcen zu ermöglichen.

Um diese genannten Weiterentwicklungen aktiv zu unterstützen, könnten Themen für studentische Arbeiten und Projekte vergeben werden.

[56] Internet: http://www.eduroam.org/ [04.12.2010]

9 Anhang

Anhang I: Fragebogen

HOCHSCHULE LAUSITZ
IFH| UNIVERSITY OF APPLIED SCIENCES
Hochschulbibliothek

Fragebogen: Identitätsmanagement in Hochschulbibliotheken

Mit diesem Formular können Sie eine Untersuchung zum Thema "Identitätsmanagement in Hochschulbibliotheken", die in unserer Hochschulbibliothek im Zeitraum von Aug. - Dez. 2010 durchgeführt wird, wirkungsvoll unterstützen. Bitte schicken Sie uns das ausgefüllte Formular bis zum **31. Juli 2010** wieder zurück. Es werden die Bestimmungen des Datenschutzes eingehalten. Alle teilnehmenden Hochschulbibliotheken können eine statistische Auswertung dieser Umfrage erhalten.

1) Erfolgt an Ihrer Hochschule ein zentrales Identitätsmanagement? ○ Ja ○ Nein

Wenn ja, ist die Hochschulbiliothek dort angebunden? ○ Ja ○ Nein

Wenn ja, welche Dienste werden darüber bereitgestellt?

a) Aktualisieren von Nutzedaten ☐

b) Authentifikation von Arbeitsstationen ☐

c) Zugang zum WLAN ☐

d) Elektronische Anmeldung ☐

e) Sonstige

Wenn nein, betreibt die Hochschulbibliothek autonom ein Identitätsmanagement? ○ Ja ○ Nein

2) Sind Arbeitszeitanteile des Bibliothekspersonals für das zentrale bzw. dezentrale Identitätsmanagement gebunden? ○ Ja ○ Nein

Wenn nein, wer ist für diese Aufgabe bibliotheksbezogen Zuständig?

Rechenzentrum ☐, Multimediazentrum ☐, Fremdfirma ☐, Sonstige

3) Haben Sie im Zuständigkeitsbereich der Hochschulbibliothek Computer-Arbeitsplätze, an welchen Ihre Nutzer Zugriff auf das Internet haben? ○ Ja ○ Nein

Wie viele solche Arbeitsplätze stellen Sie zur Verfügung?

4) Wie ist der Zugang zu diesen Arbeitsplätzen organisiert?

a) Freier Zugang für alle Besucher (keine Authentifizierung nötig) ○ Ja ○ Nein

b) Authentifizierung über Hochschul-Account für Hochschulangehörige (Mitarbeiter und Studenten) ○ Ja ○ Nein

c) Authentifizierung über Hochschulbibliotheksnutzerdatenbank (Hochschulangehörige und Externe Nutzer) ○ Ja ○ Nein

d) Kombinierte Authentifizierung aus b) und c) ○ Ja ○ Nein

Welche Software nutzen Sie dafür?

Active Directory Service ☐, webControl ☐, Radius-Server ☐, Sonstige

5) Bieten Sie Ihren Nutzern den Zugang zu elektronischen Ressourcen? ○ Ja ○ Nein

Wenn ja, zu Ebooks ☐, eJournals ☐, Fachdatenbanken ☐, Nationallizenzen ☐,
Dokumente auf eigenem Publikationsserver ☐, Sonstige

Wenn ja, wie verwalten Sie den Zugriff auf diese elektronischen Ressourcen?

a) Freier Zugang nur innerhalb Ihrer Hochschulbibliothek ○

b) Freier Zugang im Campusnetz (nur innerhalb Ihrer Hochschule) ○

c) Zugang nur über Authentifizierung ○

Wenn nur c), welche Software nutzen Sie für diese Authentifizierung?

HAN ☐, EZproxy ☐, Sonstige

6) Haben Ihre Nutzer die Möglichkeit, diese Ressourcen von außerhalb der Hochschule zu nutzen? ○ Ja ○ Nein

Wenn ja, für alle Nutzer ○ oder nur für Hochschulangehörige ○ ?

Wenn ja, welche Software nutzen Sie?

HAN ☐, EZProxy ☐, VPN Tunnel ☐, Sonstige

Anhang II: Schlüsselverzeichnis der HS Lausitz (FH)

013	Architektur	**277**	Wirt-Informatik
017	Bauingenieurwesen	**282**	Biotechnologie
021	Betriebswirtschaftslehre	**290**	Deutsch für Ausländer
022	Betriebswirtschaftslehre	**735**	Wirtschaftsing. Dual
033	Chemie	**769**	System Engineering
048	Elektrotechnik	**784**	Instrumental- Gesangspäd.
079	Informatik	**785**	Musikpädagogik
104	Maschinenbau	**796**	Bauing Dual
179	Wirtschaftsingenieurwesen	**846**	Techn. Management
200	Tech. Informatik Komm	**847**	Computational Mechanics
208	Soziale_Arbeit	**849**	Kommunikations- E-technik
213	Versorgungstechnik	**850**	Klimagerechtes Bauen
215	Medizinische Technik	**855**	Naturstoffchemie
226	Verfahrenstechnik	**856**	Architektur Architektura
232	Sozialmanagement	**933**	Physiotherapie Dual
233	Physiotherapie Dual	**B53**	Sozialarbeit (BB)
234	Gerontologie	**T13**	Architektur Teilzeit
253	Sozialarbeit -pädagogik		

Tab. 1: Schlüsselverzeichnis HS Lausitz (FH) in Tabelle d00keyver

Anhang III: Softwarespezifikation SQL2SQL

Dieses Programm soll Daten aus einer SQL-Datenbank in eine andere übertragen. Hierbei kann es sich um unterschiedliche Server mit unterschiedlichen SQL-Datenbanktypen handeln. Einige JDBC Treiber sollen bereits eingebunden sein, z.B. DB2, MS-SQL, MySQL, Oracle, PostgreSQL und Sybase. Die Einstellungen der Kommunikation, der SQL-Statements, des Quell- und Zielsystems soll in einer XML-Steuerdatei abgelegt werden. Für unterschiedliche Aufgaben muss es möglich sein, unterschiedliche XML-Steuerdateien zu erzeugen. Dieses Programm kann auf einem dritten unabhängigen Rechner ausgeführt werden. Dieser führt per cron-Jobs zu definierten Zeiten dieses Programm mit der jeweiligen XML-Steuerdatei aus.

Export/Import sind dabei frei definierbare SQL-Querys (select/insert). Diese sind vom Anwender aufeinander abzustimmen. Es findet keine Datenmanipulation mit den exportierten Daten statt. Export-Daten werden in eine temporären Tabelle zwischengespeichert. Diese dient für den Datenimport (insert) in das Zielsystem. Vor diesem Datenimport soll optional auf dem Zielsystem ein SQL Query ausführbar sein (z.B.: create, update oder delete).

Zusammenfassung:

- Quell- und Zielsystem Konfiguration:
    - Datenbank-URL,
    - Datenbank-Treiber,
    - Datenbank-Name,
    - Datenbank-Nutzer,
    - Datenbank-Passwort (möglichst md5),
    - Datenbank-Verbindungstest,
    - SQL - Query Quellsystem: select
Zielsystem: insert
    - Option: vor Import SQL-Query (create, delete, update)
- ausführbare jar-Datei – mit XML-Config-File
- log Datei mit SQL-Ergebnis
- grafische Oberfläche Gui zum einfachen editieren der XML-Config-Files

10 Literaturverzeichnis

[BibDi2000]
Checkliste „Internet in den Universitätsbibliotheken", BIBLIOTHEKSDIENST 34. Jg. (2000),H.9
Internet: http://bibliotheksdienst.zlb.de/2000/2000_09_Recht02.pdf [20.11.2010]

[Borel]
Borel, Frank: Einführung in Shibboleth, Berlin, 2007
Internet: https://www.aai.dfn.de/fileadmin/documents/WS5/shibboleth-einfuehrung-borel.pdf
[31.10.2010]

[BuB0210]
Wirts, Hans Christian: Schnelle Schnittstelle zum Kunden, in BuB 62 (2010) 2

[DBV2006]
Talke, Armin: Stellungnahme der DBV-Rechtskommission, Bibliotheksdienst 40. Jg. (2006), H. 8/9
Internet: http://www.zlb.de/aktivitaeten/bd_neu/heftinhalte2006/Recht01080906.pdf

[DBV2010]
Talke, Armin: Rechtliche Aspekte von Internet-Dienstleistungen der Bibliotheken (Haftung / Vorratsspeicherung) 04.08.2010

Internet:http://www.bibliotheksverband.de/fileadmin/user_upload/Kommissionen/Kom_Recht/Rechtsinformationen/04082010_Rechtliche_Aspekte_von_Internet-Dienstleistungen.pdf
[20.11.2010]

[DINI ÖA]
Empfehlungen für Einrichtung von öffentlichen Computer- oder Netzarbeitsplätzen, Göttingen, 2004
Internet: http://www.dini.de/fileadmin/ag/oecap/oecnap_102004_final.pdf [20.11.2010]

[EZP]
EZProxy [OCLC - Bibliotheks-managementsysteme und -services]
Internet: http://www.oclc.org/de/de/ezproxy/ [31.10.2010]

[FGMwC3.7]
SISIS-SunRise webControl V3.7 Freigabemitteilung, Oberhaching, 2009

[Fisch]
Fischer, Peter / Hofer, Peter: Lexikon der Informatik, Heidelberg, 2008
E-Book: http://dx.doi.org/10.1007/978-3-540-72550-3

[Geier]
Geier , Bernhard: Realisierung und Einführungskonzept einer standortübergreifenden Vereinheitlichung der Benutzerverwaltung mit LDAP, Diplomarbeit, FH Ingolstadt, 2005
Internet: http://www2.fh-augsburg.de/~hhoegl/da/da-30/Diplomarbeit.pdf [30.11.2010]

[Gragert]
Bibmarks Blog Archive OCLC erwirbt EZProxy
Internet: http://blog.gragert.de/?p=22 [31.10.2010]

[HAN]
Hidden Automatic Navigator
Internet: http://www.hh-han.com/de/ [31.10.2010]

[HS2010]
Statistik Internetseite HS Lausitz Hochschulbibliothek
Internet: „http://www.hs-lausitz.de/hochschulbibliothek/unsere-hochschulbibliothek/statistik/bestand.html“ [31.10.2010]

[Huber]
Huber, Roland: openLDAP Verzeichnisdienst, 2002
Internet: http://www.books.ignix.ru/DAEMONS/LDAP/Open_Ldap_DE.pdf [31.10.2010]

[IDM-C]
OCLC IDM-CONNECTOR V3.7PL2 Administrationshandbuch, Oberhaching, 2010

[IFLA]
Richtlinien zum IFLA/UNESCO Internet-Manifest, 2006
Internet: http://archive.ifla.org/faife/policy/iflastat/Internet-ManifestoGuidelines-de.pdf
[22.11.2010]

[iFQ2010]
iQ Übersicht Fachhochschulen in Deutschland
Internet: http://www.forschungsinfo.de/iq/institutionen/FHliste_men.asp [20.08.2010]

[IM HS]
Bode, Arndt / Borgeest, Rolf (Herausgeber): Informationsmanagement in Hochschulen, Heidelberg, 2010
E-Book: http://dx.doi.org/10.1007/978-3-642-04720-6

[Java]
java-ldap-api: Java LDAP Client API Project
Internet: https://java-ldap-api.dev.java.net/ [30.10.2010]

[Kappes]
Kappes, Martin: Netzwerk- und Datensicherheit, Wiesbaden, 2007
E-Book: http://dx.doi.org/10.1007/978-3-8351-9202-7

[Klünter]
Klünter, Dieter / Laser, Jochen: LDAP verstehen, OpenLDAP einsetzen, Heidelberg, 2003

[Lange]
Langenstein, Annette: Einsatz des IDM-Connector an der UB Heidelberg, Beitrag des 33. SISIS-Anwendertreffens, Nürnberg, 2009
Internet: http://sv.ub.uni-bayreuth.de/ssv/AG/SAT/sat_20091202_files/Langenstein_IDM-ubhd.pdf [18.11.2010]

[Liebel]
Liebel, Oliver / Ungar, John Martin: OpenLDAP, Bonn, 2006

[Lipp]
Lipp, Manfred: VPN-virtuelle Private Netzwerke, München, 2001

[PHP]
PHP: ldap_add - Manual
Internet: http://www.php.net/manual/de/function.ldap-add.php [10.10.2010]

[Reichw]
Reichwald, Ralf: Mobile Kommunikation: Wertschöpfung, Technologien, neue Dienste, Wiesbaden, 2002

[Schoen]
Schoenherr, Oliver: Konzeption und Implementierung eines Java-Backends für einen LDAP-Server, Diplomarbeit, Berlin, 1999
Internet: https://users.informatik.haw-hamburg.de/~schmidt/thesis/oliver_schoenherr.pdf

[Schwoch]
Schwoch, Dietrich / Küveler, Gerd: Informatik für Ingenieure und Naturwissenschaftler2, Wiesbaden, 2007

[Seifert]
Seifert, Robin: Entwicklung einer generischen Software für eine automatisierte Datenreplikation zwischen Datenbanken und Active Directory, Diplomarbeit, Senftenberg, 2009

[Siman]
Simanowski, Jörg: Zugang zu elektronischen Ressourcen für externe Benutzer in wissenschaftlichen Bibliotheken : Konzeption und praktische Anwendung, Masterarbeit, Berlin, 2008
Internet: http://www.ib.hu-berlin.de/~kumlau/handreichungen/h241/ [28.11.2010]

[SISISwC2005]
SISIS-SunRise webControl - der maßgeschneiderte Internet-Zugang für Ihre Nutzer, Oberhaching, 2005
Internet: http://www.sisis.de/dasat/images/0/100520-webcontrol.pdf [05.10.2010]

[SOI]
Abschlussbericht: Service-orientierte IT-Infrastruktur an niedersächsischen Hochschulen, Hannover, 2005
Internet: http://soi.lanit-hrz.de/export/sites/default/de/download/soi-abschlussbericht.pdf [18.11.2010]

[Springer2008]
E-Books – die Sicht der Nutzer
Internet: http://www.springer.com/cda/content/document/cda_downloaddocument/V2628+WhitePaper_5_DACH.pdf?SGWID=0-0-45-740298-0 [31.10.2010]

[Starick]
Starick, Martin: Entwicklung einer zentralen Benutzerdatenverwaltung als Teil eines Identity Management Systems unter Verwendung von J2EE-Technologien und Open Source Framework, Diplomarbeit, Senftenberg, 2008

[UZH.CH]
Milosevic, Nenad: UZH - ZInfo - Zeitschrift der Informatikdienste - EZproxy: Vereinfachter Zugang von Ausserhalb ins Netz der Universität Zürich
Internet: http://www.id.uzh.ch/cl/zinfo/zinfo0027/kattipps/ezproxy-27.html [31.10.2010]